SYNGRESS®

PCI Compliance

Understand and Implement Effective PCI Data Security Standard Compliance

- Avoid Stiff Penalties from the Credit Card Industry
- Understand the Risks of Non-Compliance and the Benefits of Compliance
- Complete Coverage of Protecting Cardholder Data, Stored Data, and Data in Transit

Tony Bradley Technical Editor
James D. Burton Jr.
Dr. Anton Chuvakin
Anatoly Elberg
Brian Freedman
David King
Scott Paladino
Paul Schooping

Visit us at

www.syngress.com

Syngress is committed to publishing high-quality books for IT Professionals and delivering those books in media and formats that fit the demands of our customers. We are also committed to extending the utility of the book you purchase via additional materials available from our Web site.

SOLUTIONS WEB SITE

To register your book, visit www.syngress.com/solutions. Once registered, you can access our solutions@syngress.com Web pages. There you may find an assortment of value-added features such as free e-books related to the topic of this book, URLs of related Web sites, FAQs from the book, corrections, and any updates from the author(s).

ULTIMATE CDs

Our Ultimate CD product line offers our readers budget-conscious compilations of some of our best-selling backlist titles in Adobe PDF form. These CDs are the perfect way to extend your reference library on key topics pertaining to your area of expertise, including Cisco Engineering, Microsoft Windows System Administration, CyberCrime Investigation, Open Source Security, and Firewall Configuration, to name a few.

DOWNLOADABLE E-BOOKS

For readers who can't wait for hard copy, we offer most of our titles in downloadable Adobe PDF form. These e-books are often available weeks before hard copies, and are priced affordably.

SYNGRESS OUTLET

Our outlet store at syngress.com features overstocked, out-of-print, or slightly hurt books at significant savings.

SITE LICENSING

Syngress has a well-established program for site licensing our e-books onto servers in corporations, educational institutions, and large organizations. Contact us at sales@syngress.com for more information.

CUSTOM PUBLISHING

Many organizations welcome the ability to combine parts of multiple Syngress books, as well as their own content, into a single volume for their own internal use. Contact us at sales@syngress.com for more information.

SYNGRESS®

SYNGRESS®

PCI Compliance

Implementing Effective PCI Data Security Standards

Tony Bradley Technical Editor
James D. Burton Jr.
Dr. Anton Chuvakin
Anatoly Elberg
Brian Freedman
David King
Scott Paladino
Paul Shcooping

KEY	SERIAL NUMBER
001	HJIRTCV764
002	PO9873D5FG
003	829KM8NJH2
004	BAL923457U
005	CVPLQ6WQ23
006	VBP965T5T5
007	HJJJ863WD3E
008	2987GVTWMK
009	629MP5SDJT
010	IMWQ295T6T

PUBLISHED BY
Syngress Publishing, Inc.
Elsevier, Inc.
30 Corporate Drive
Burlington, MA 01803

PCI Compliance: Understand and Implement Effective PCI Data Security Standard Compliance

Printed in the United States of America
1 2 3 4 5 6 7 8 9 0
ISBN-13: 978-1-59749-165-5

Publisher: Amorette Pedersen
Acquisitions Editor: Andrew Williams
Technical Editor: Tony Bradley
Cover Designer: Michael Kavish

Page Layout and Art: Patricia Lupien
Copy Editor: Judy Eby
Indexer: Odessa&Cie

For information on rights, translations, and bulk sales, contact Matt Pedersen, Commercial Sales Director and Rights, at Syngress Publishing; email m.pedersen@elsevier.com.

Technical Editor

Tony Bradley (CISSP-ISSAP) is the Guide for the Internet/Network Security site on About.com, a part of The New York Times Company. He has written for a variety of other Web sites and publications, including *BizTech Magazine*, *PC World*, SearchSecurity.com, WindowsNetworking.com, *Smart Computing* magazine, and *Information Security* magazine. Currently a Security Consultant with BT INS in Houston, TX, Tony performs a wide range of information security tasks and functions. Tony has driven security policies and technologies for antivirus and incident response for Fortune 500 companies, and he has been network administrator and technical support for smaller companies.

Tony is a CISSP (Certified Information Systems Security Professional) and ISSAP (Information Systems Security Architecture Professional). He is Microsoft Certified as an MCSE (Microsoft Certified Systems Engineer) and MCSA (Microsoft Certified Systems Administrator) in Windows 2000 and an MCP (Microsoft Certified Professional) in Windows NT. Tony is recognized by Microsoft as an MVP (Most Valuable Professional) in Windows security.

On his About.com site, Tony has on average over 600,000 page views per month and over 30,000 subscribers to his weekly newsletter. He created a 10-part Computer Security 101 Class that has had thousands of participants since its creation and continues to gain popularity through word of mouth. In addition to his Web site and magazine contributions, Tony was also author of *Essential Computer Security: Everyone's Guide to E-mail, Internet, and Wireless Security* (ISBN: 1597491144), coauthor of *Hacker's Challenge 3* (ISBN: 0072263040) and a contributing author to *Winternals: Defragmentation, Recovery, and Administration Field Guide* (ISBN: 1597490792), *Combating Spyware in the Enterprise* (ISBN: 1597490644) *Syngress Force 2006 Emerging Threat Analysis: From Mischief to Malicious* (ISBN: 1597490563), and *Botnets: The Killer Web Applications* (ISBN: 1597491357).

Acknowledgements

Taking a book from a concept and a vision to a finished, hard copy product is not an easy task. I want to thank Amy Pedersen of Syngress for staying on top of myself and the rest of the writers to keep the project on track. Amy had to put in some extra effort to juggle and replace authors as the project progressed, and her efforts are greatly appreciated. I also want to thank all of the contributing authors. Everyone has day jobs and personal lives and making a commitment to contribute to a book is often a challenge.

Dedication

This work is dedicated to my family. My wife Nicki, and my children Jordan, Dalton, Paige, Teegan, Ethan, Noah and Addison, as well as my in-laws have always been very proud and supportive of my efforts. Without their backing, I would not have the successes that I have had.

Contributors

James D. Burton Jr., CISSP, CISA, CISM, GSNA, is a Sr. I.T. Security Professional with over 12 years in the field. He is a well-known subject matter expert in the areas of IT security, information assurance and IT audit, and has worked as a consultant, trainer, and an adjunct professor. He has worked on projects or trained for major companies and organizations including Citibank, Global Healthcare Exchange, Idea Integration, Agilent Technologies, Northrop Grumman, SRS Technologies, Secure Banking Services, IP3, Inc. and the U.S. Marine Corps. He was an adjunct professor for Colorado Technical University, where he taught courses on foundations of security and security management at the bachelor and master level. James has an M.S. in Computer Science from Colorado Technical University (2002). He was also a contributing author to *Cisco Security Professional's Guide to Secure Intrusion Detection Systems* (Syngress, 2003). James is currently working with Secure Banking Services performing IT audit services to the financial industry and is a trainer for IP3, Inc.

Dr. Anton Chuvakin, GCIA, GCIH, GCFA (http://www.chuvakin.org) is a recognized security expert and book author. In his current role as a Director of Product Management with LogLogic, a log management and intelligence company, he is involved with defining and executing on a product vision and strategy, driving the product roadmap, conducting research as well as assisting key customers with their LogLogic implementations. He was previously a Chief Security Strategist with a security information management company. A frequent conference speaker, he also represents the company at various security meetings and standards organizations. He is an author of a book "Security Warrior" and a contributor to *Know Your Enemy II*, *Information Security Management Handbook,* and *Hacker's Challenge 3*. Anton also published numerous papers on a broad range of security subjects. In his spare time he maintains his security portal http://www.info-secure.org and several blogs. Aton would like to thank Jason Chan for his help reviewing my chapters' contents. Finally, Anton would like to dedicate his book chapters to his lovely wife, Olga.

Anatoly Elberg, QSA, CISSP, has over 10 years of experience and is an accomplished security professional. His focus includes IT governance, regulatory compliance, and risk management. Anatoly has implemented strategic information security management programs for large technology, financial, retail, and telecommunications companies. Currently he is a Principal Consultant and a regional security practice lead at BT INS. Anatoly has been working with Visa's Cardholder Information Security Program (CISP) requirements since 2004, and is certified by the PCI Security Standards Council as a Qualified Security Assessor (QSA). In addition, Anatoly holds the CISSP, MCSE, CHSP, NSA IAM, and NSA IEM certifications. He has a bachelors degree from the University of Texas at Austin, and is a member of the Information Systems Auditing and Controls Association (ISACA).

Brian Freedman (CISSP, MCSE, CCEA, CCNA) is the Director of Infrastructure Services and Security with Benefitfocus. Benefitfocus is the leader in software and services for the healthcare benefits market headquartered in Charleston, South Carolina. Brian manages the Infrastructure that runs the applications Benefitfocus creates. As Benefitfocus has grown Brian has also taken on the role of the compliance officer for the organization where he has lead compliance efforts for both the Payment Card Industry Data Security Standards and HIPAA. His specialties include Cisco networking, voice over IP and security, Microsoft Windows Servers, Microsoft Exchange, Data Center Design and Maintenance, and HIPAA and PCI DSS compliance efforts.

Brian holds a bachelor's degree from the University of Miami, and currently resides in Charleston, SC with his wife Starr, and children Myles, Max, and Sybil.

David King (CISSP) is the CEO of Remote Checkup, Inc. He has worked with credit card industry security standards since 2004. As the IT directory of an e-commerce company he helped them comply with these standards. Since then he built a company from the ground up that has become a PCI approved scanning vendor. He currently consults with companies to help them meet PCI requirements using open source solutions whenever possible. Leveraging his background in system administration and coding, he also helps companies develop custom solutions that help them

bridge gaps in compliance. David has taught courses in system administration, networking, and security at a local college. He holds a bachelor's degree in computer science from Brigham Young University and currently lives in American Fork, UT with his family, Megan and Sabrina.

Scott Paladino (CISSP) is a security architect with EDS (www.eds.com), a leading global technology services company. He is the Engineering Organization Leader at EDS supporting identity, access, and other security solutions across a variety of industries.

Paul Schooping (CISSP) is a Security Engineer for a leading global technology services company. He currently participates in the design, implementation and support of global security and privacy solutions. Paul's background includes experience as the Global Antivirus and Vulnerability Manager for a Fortune 500 Company and the development of an enterprise Emergency Security Response Team. His specialties include Antivirus, vulnerability assessment, reverse engineering of malware, and encryption technologies. Paul holds a bachelors degree in psychology and formerly served in multiple youth ministry positions. He currently resides in Rochester, NY with his wife Margaret, and two daughters – Rachel and Rebecca.

Contents

Chapter 1

About PCI and This Book

Introduction

There are plenty of standards and regulations out there. If you are a publicly traded company in the United States, you must adhere to the (SOX) mandates. If you are in the health care industry your network must comply with the Health Insurance Portability and Accountability Act (HIPAA) standards. The list goes on.

The bottom line is that organizations need to secure and protect their networks. In some cases, weak network security may only affect the company. However, when the data on the corporate network contains personal information about patients, customers, or employees, a breach of security can have implications far beyond the company.

The credit card industry banded together to develop the Payment Card Industry (PCI) Data Security Standards (DSS) to ensure that credit card customer information is adequately protected and to protect the industry. Breaches of customer information lead to lost money and damaged reputations, and the credit card industry wants to protect itself from financial loss or eroded consumer confidence in credit cards as a means of transacting money.

This book will explain the PCI DSS guidelines to you. However, it will do so in a broader, more holistic approach. The goal of this book is to not only teach you the PCI DSS requirements, but to help you understand how the PCI DSS requirements fit into an organization's network security framework, and how to effectively implement network security controls so that you can be both compliant and secure.

Who Should Read This Book?

Every company that accepts credit card payments, processes credit card transactions, stores credit card data, or in any other way touches personal or sensitive data associated with credit card payment processing, is affected by the PCI DSS. Virtually all businesses, no matter how big or how small, need to understand the scope of the PCI DSS and how to implement network security that is compliant with the PCI guidelines, or face penalties or the possibility of having their merchant status revoked and potentially being banned from accepting or processing credit cards.

Even with such a broad audience compelled to comply with the PCI DSS, this book had to be written for a specific technical level. The book could have been written in very simple terms in order to educate the general population about PCI DSS. We could have written an in-depth technical tome providing every bit of detail a network engineer or security administrator might need to configure and

implement compliance. This book is more of a strategic business guide to help executive management understand the implications of PCI DSS and what it takes to be compliant

This book is for the Information Technology (IT) managers and company executives who need to understand how the PCI DSS apply to them. This book is for the small- and medium-size business that doesn't have an IT department to delegate to. For organizations that need to grasp the concepts of PCI DSS and how to implement an effective security framework that is compliant. This book is intended as an introduction to PCI, but with a deeper and more technical understanding of how to put it into action.

Organization of the Book

Each chapter of the book is designed to provide you the information you need to know in a way that you can easily understand and apply. To aid in that goal, the chapters have a consistent look and feel and are each made up of the same basic sections, listed here.

Solutions In This Chapter

At the beginning of each chapter is a bulleted list called Solutions In This Chapter. This list shows you a high-level overview of the concepts that are covered in this chapter and what you can expect to learn.

Summary

Every chapter has a summary. As the name implies, the summary summarizes the information covered in the chapter and provides a brief recap of the concepts discussed to reinforce what you read, or to help you identify areas that you may need to re-read if you don't feel you understand them yet.

Solutions Fast Track

The Solutions Fast Track provides a bulleted outline of the pertinent points and key information covered in the chapter. This section can be used as a sort of study guide or reminder system to help trigger your brain to recall the information or to review in one short list the key points from the chapter

Frequently Asked Questions

Frequently asked questions contain questions designed to clarify areas of potential confusion from the chapter or reinforce the information that was covered. This section can also serve as a sort of mini-quiz to demonstrate that you grasp the concepts and information discussed in the chapter.

Chapter Descriptions

This section provides a brief description of the information covered in each chapter:

- **Chapter 1: Foreword** A discussion of the state of credit card data security and how this book came about
- **Chapter 2: Introduction** A brief look at the target audience of the book, as well as an overview of the chapter formats and content.
- **Chapter 3: Why PCI Is Important** An overview of PCI DSS and why the credit card industry was compelled to create it. This chapter also includes some discussion about the benefits of PCI DSS compliance and the risks and consequences of non-compliance.
- **Chapter 4: Building and Maintaining a Secure Network** The first step in protecting any kind of data, and for PCI DSS compliance, is to have a secure network in the first place. This chapter discusses the basic components of a secure network and lays the foundation for building the rest of your PCI DSS compliance.
- **Chapter 5: Protect Cardholder Data** This chapter explains how to protect data that is stored on your network, as well as how to protect data while it is in transit. It also covers access controls and logging so that you can determine who accessed a given file and whether or not they were authorized to do so.
- **Chapter 6: Logging Access and Events** A discussion about how to configure logging and event auditing to capture the information you need to be able to demonstrate and maintain PCI compliance.
- **Chapter 7: Strong Access Control** This chapter covers one of the most important aspects of PCI DSS compliance- access controls. The information

in this chapter includes the need to restrict access to only those individuals that need it, as well as restricting physical access to computer systems.

- **Chapter 8: Vulnerability Management** Performing vulnerability assessments to identify weaknesses in systems and applications, and how to mitigate or remediate the vulnerabilities to protect and secure your data.
- **Chapter 9: Monitoring and Testing** How to monitor your network and test your security controls to ensure your network is protected and compliant.
- **Chapter 10: How To Plan a Project To Meet Compliance** An overview of the steps involved and tasks necessary to implement a successful PCI compliance project. This chapter includes a discussion of the basic elements that should be included in any future projects as well to proactively ensure they are PCI compliant.
- **Chapter 11: Responsibilities** An effective incident response process requires that the groups and individuals responsible for responding understand their roles. This chapter discusses the different components of incident response and how to respond effectively to breaches of PCI DSS.
- **Chapter 12: Planning to Fail Your First Audit** Understand that an auditor is there to work with you to achieve compliance. They are not the enemy. This chapter explains how to use the findings from a failed audit to ensure compliance.
- **Chapter 13: You're Compliant! Now What?** This chapter covers the details you need to keep in mind once you have achieved compliance. Security is not as simple as just getting it implemented. You have to monitor and maintain it. This chapter contains information about ongoing training and periodic reviews, as well as how to conduct a self-audit to ensure continued compliance.

Chapter 2

Introduction to Fraud, ID Theft, and Regulatory Mandates

By Tony Bradley, CISSP-ISSAP,
Microsoft MVP-Windows Security
BT INS Security Consultant

Credit card fraud and identity theft are both epic problems that continue to grow each year. Certainly, credit card fraud and identity theft pre-date the age of the Internet. It is an ironic fact that the things that make your life easier, improve efficiency, and make things more convenient, also make crime easier, efficient, and more convenient.

Criminals have gone high-tech and they have discovered that there is a significant amount of money to be acquired with very little risk. Hacking a company database or orchestrating a phishing attack while sitting in your pajamas eating chocolate ice cream in the living room of your house has much more appeal than robbing banks or convenience stores, and the risk of getting shot or killed is much lower. Depending on the company being targeted, the sophistication of the attack, and sometimes sheer luck, the high-tech crime may also be significantly more lucrative than traditional armed robbery.

Malicious software (malware) and cyber-criminals are not the only threat. Sadly, the very companies and organizations that are entrusted with sensitive information are often to blame. Consumers and businesses are faced with a wide variety of threats to their data and personal information on any given day. Spyware, phishing attacks, and robot networks (botnets) are all computer attacks that are on the rise and pose a significant threat to users as they connect to the Web and use their computers. However, those threats pale in comparison with the amount of personally identifiable information and sensitive data that has been compromised through carelessness or negligence by corporations.

According to some sources, more than 50 million individual records were exposed in 2005, through the loss of mobile devices or portable storage media, or by attackers gaining access to the corporate network and extracting the data themselves. A security breach at CardSystems in June 2005, was responsible for 40 million of the 50 million total. Early in 2007, a security breach at TJX Companies, the parent of retail establishments such as T.J. Maxx, Bob's, Marshall's, HomeGoods, and A.J. Wright, may potentially have exposed more credit information and individual account data than even the 40 million records compromised by CardSystems data. Some estimates place the TJX breach at over 50 million compromised accounts by itself.

In an era when more consumers are using computers and the Internet to conduct business and make purchases, and more companies are storing more data, it is more important than ever that the proper steps are taken to secure and protect personally identifiable information and other sensitive data. It is bad for companies, individuals, and the economy at large if consumer confidence is eroded by having their personal information exposed or compromised.

The information security field has a number of laws and regulations to adhere to. Depending on what industry a company does business in, they may fall under Sarbanes-Oxley (SOX), the Gramm-Leach Bliley Act of 1999 (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), and other regulatory mandates, or some combination thereof. However, as evidenced by the volume and continuing occurrence of data compromise and exposure, many organizations still fail to enforce adequate security measures.

These breaches are often targeted at consumer credit card information, and threatened to tarnish the reputation of the credit card industry, so the major credit card vendors banded together to develop the Payment Card Industry (PCI) Data Security Standards (DSS). In essence, the credit card industry has taken proactive steps to assure the integrity and security of credit card data and transactions and maintain the public trust in credit cards as a primary means of transacting money. If you want to accept credit cards as payment or take part in any step of the processing of the credit card transaction, you must comply with the PCI DSS or face stiff consequences.

Unlike SOX or HIPAA, the PCI DSS are not a law; however, in many ways, they are more effective. Non-compliance won't land you in jail, but it can mean having your merchant status revoked. For some organizations, losing the ability to process credit card payments would drastically affect their ability to do business and possibly even bring about the death of the company.

There is nothing extraordinary or magical about the PCI DSS requirements, though. The guidelines spelled out are all essentially common sense that any organization should follow without being told. Even so, some of the requirements leave room for interpretation and complying with PCI DSS can be tricky.

As with any information security regulation or guideline, you need to keep your eye on the ultimate goal. When executing a compliance project, some organizations follow the letter, rather than the spirit of the requirements. The end result may be that they were able to check off all of the boxes on the checklist and declare their network compliant, yet not be truly secure. Remember, if you follow the requirements and seek to make your network as secure as possible, you are almost guaranteed to be compliant. But, if you gloss over the requirements and seek to make your network compliant, there is a fair chance that your network could still be insecure.

The major retailers and larger enterprises are well aware of the PCI DSS. They have dedicated teams that can focus on security and on PCI DSS compliance. They have the resources and the budget to bring in third-party auditors to assess and remediate issues. The scope of PCI DSS impacts almost every business, from the

largest retail megastores down to a self-employed single mother working from her home computer. If the business accepts, processes, transmits, or in any other way handles credit card transactions, they must comply with PCI DSS.

I created this book to give small and medium organizations something they can work with. It is not simply a rehash of the PCI DSS requirements. You can get the latest copy of the standard from PCI Co and read the requirements yourself for free. This book takes a more holistic approach. I have structured the book to address the major areas of network management and information security, and how to effectively implement processes and technologies that will make your organization more secure and compliant with PCI DSS at the same time.

The purpose of this book is to provide an overview of the components that make up the PCI DSS and to provide you with the information you need to know to get your network PCI DSS compliant and keep it that way. Each major area of security covered by the PCI DSS are discussed in some detail along with the steps you can take to implement the security measures on your network to protect your data.

The team of authors that have assisted on this project are each established information security professionals. They have been there and done that, and have acquired wisdom through trial and error. Their experience is shared here to help you implement effective solutions that are both secure and compliant.

Chapter 3

Why PCI Is Important

Solutions in this Chapter:

- What is PCI?
- Overview of PCI Requirements
- Risks and Consequences
- Benefits of Compliance

- ☑ Summary
- ☑ Solutions Fast Track
- ☑ Frequently Asked Questions

Introduction

Chances are if you picked up this book you already know something about the Payment Card Industry (PCI). This chapter covers everything from the conception of the cardholder protection programs by the individual card brands to the founding of the PCI Security Standards Council. Why? To make sure that you have not been misled and that you use the terminology in the right context. Also, many of the questions people ask have their origins in the history of the program, so it only makes sense that we start at the beginning.

What is PCI?

PCI is not a regulation. The term PCI stands for Payment Card Industry. What people are referring to when they say PCI is actually the PCI Data Security Standard (DSS), currently at version 1.1. However, to make things easy, we will continue to use the term PCI to identify the industry regulation.

Who Must Comply With the PCI?

In general, any company that stores, processes, or transmits cardholder data must comply with the PCI. In this book, we are primarily concerned with merchants and service providers. The merchants are pretty easy to identify—they are the companies that accept credit cards in exchange for goods or services. However, when it comes to service providers, things get a bit trickier. A service provider is any company that processes, stores, or transmits cardholder data, including companies that provide services to merchants or other service providers.

NOTE

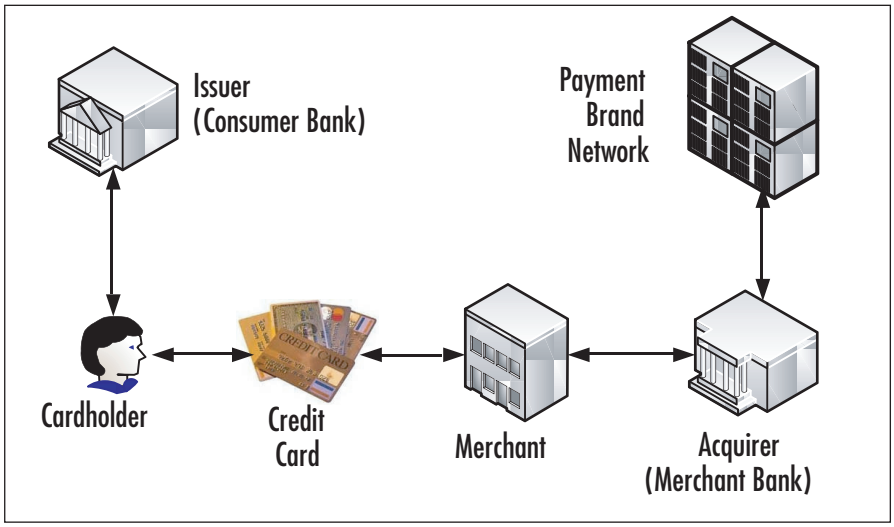
The following terms are used throughout this book.

- **Cardholder** The legal owner of the credit card.
- Cardholder Data At a minimum includes the primary account number (PAN), but also may include the cardholder name, service code, or expiration data when stored in conjunction with the account number.
- Storage of Cardholder Data **Any retention of cardholder data on** digital or analog media. Not limited to digital information. Often excludes temporary retention for troubleshooting or customer service purposes.

- **Processing of Cardholder Data** Any manipulation of cardholder data by a computing resource or on physical premises. Not limited to digital information.
- **Transmission of Cardholder Data** Any transfer of cardholder data through a part of the computer network or physical premises. Not limited to digital information.
- **Acquirer (Merchant) Bank** The bank that processes a merchant's transactions; can be a card brand (in the case of American Express, Discover, and JCB).
- **Issuer Bank** The bank that issues the credit card.
- **Card Brand** Visa, MasterCard, American Express, Discover, or JCB.
- **Authorization** Request to charge a particular amount to the credit card, and a receipt of approval.
- **Clearing** Presentation of a transaction to a payment card brand.
- **Settlement** A process of transferring funds between an acquiring bank and an issuing bank.
- **Open Payment System** A system where the card brand does not act as an acquirer; applies to Visa and MasterCard.
- **Closed Payment System** A system where the card brand acts as an acquirer; applies to American Express, Discover, and JCB.
- **Merchant** Any company that accepts credit cards in exchange for goods or services.
- **Service Provider** Any company that processes, stores, or transmits cardholder data, including companies that provide services to merchants or other service providers.
- **Payment Gateway** A service provider that enables payment transactions, specifically located between the merchant and the transaction processor.
- **Third Party Processor (TPP)** A service provider that participates in some part of the transaction process.
- **Data Storage Entity (DSE)** A service provider that is not already a TPP.
- **Card Validation Value (CVV)** A special value encoded on the magnetic stripe, designed to validate that the credit card is physically present.
- **Card Validation Code (CVC)** MasterCard's equivalent to CVV.
- **Card Validation Value 2 (CVV2)** A special value printed on the card, designed to validate that the credit card is physically present.
- **Card Validation Code 2 (CVC2)** MasterCard's equivalent to CVV2.
- **Card Identification Data (CID)** American Express' and Discover's equivalent to CVV2.

Figure 3.1 shows the relationship among the different parties.

Figure 3.1 Payment Industry Terminology



There are different levels of merchants and service providers. Tables 3.1 and 3.2 show the breakdown.

Table 3.1 Merchant Levels

Merchant Level	Description
Level 1	Any merchant that processes more than 6 million Visa or MasterCard transactions annually. Any merchant that processes more than 2.5 million American Express transactions annually.
Level 2	Any merchant that processes between 1 million and 6 million Visa transactions annually. Any merchant that processes more than 150 thousand MasterCard e-commerce transactions annually. Any merchant that processes between 50 thousand and 2.5 million American Express transactions annually.
Level 3	Any merchant that processes between 20 thousand and 1 million Visa e-commerce transactions annually. Any merchant that processes more than 20 thousand MasterCard e-commerce transactions annually. Any merchant that processes less than 50 thousand American Express transactions annually.

Continued

Table 3.1 continued Merchant Levels

Merchant Level	Description
Level 4	All other Visa and MasterCard merchants.

NOTE

Visa Canada levels may differ. Discover and JCB do not classify merchants based on transaction volume. Contact the payment brand for more information.

Table 3.2 Service Provider Levels

Level	MasterCard	Visa USA
Level 1	All third-party providers (TPPs) All data storage entities (DSEs) that store, process, or transmit cardholder data for Level 1 and Level 2 merchants	Any VisaNet processor All payment gateways
Level 2	All DSEs that store, process, or transmit cardholder data for Level 3 merchants	Any service provider that stores, processes, or transmits one million or more Visa accounts or transactions annually
Level 3	All other DSEs	Any service provider that stores, processes, or transmits less than one million Visa accounts or transactions annually

NOTE

American Express, Discover, and JCB do not classify service providers based on transaction volume. Contact the payment brand for more information.

These levels exist mainly for ease of compliance validation. It is a common misconception that the compliance requirements vary among the different levels. Both merchants and service providers must comply with the entire DSS, regardless of the level. Only verification processes and reporting vary.

It is possible for a company to be a merchant and a service provider at the same time. If this is the case, the circumstances should be noted, and the compliance must be validated at the highest level. In other words, if a company is a Level 3 merchant and a Level 2 service provider, the compliance verification activities should adhere to the requirements for a Level 2 service provider.

Dates to Remember

When do I need to be compliant? Some of you recall receiving a letter from your company's bank or a business partner that had a target compliance date. This date may or may not be aligned with the card brands' official dates. This is because the card brands may not have a direct relationship with you, and are working through the business chain. When in doubt, always follow the guidance of your legal department that has reviewed your contracts.

Barring unusual circumstances, the effective compliance deadlines have long passed. Various predecessor versions of the PCI 1.1 standard had unique dates associated with them, so if your compliance efforts have not been aligned to the card brand programs, you are way behind the curve and will likely not get any sympathy from your bank.

Table 3.3 Compliance Dates for Merchants

Level	American Express	MasterCard	Visa USA
Level 1	October 31, 2006	June 30, 2005	June 30, 2004
Level 2	March 31, 2007	June 30, 2004	June 30, 2007
Level 3	N/A	June 30, 2005	June 30, 2005
Level 4	N/A	N/A	N/A

NOTE

Visa USA's target compliance date of June 30, 2007 is applicable to new Level 2 merchants only. If you have not changed levels, you probably do not qualify. Visa Canada, Discover, and JCB compliance dates for merchants are not well defined. Please check with your acquirer for more information.

Table 3.4 Compliance Dates for Service Providers

Level	MasterCard	Visa USA
Level 1	June 30, 2005	September 30, 2004
Level 2	June 30, 2005	September 30, 2004
Level 3	June 30, 2005	September 30, 2004

NOTE

American Express, Visa Canada, Discover, and JCB compliance dates for service providers are not well defined. Please check with your acquirer for more information.

Compliance Process

Depending on your company's merchant or service provider level, you will either need to go through an annual on-site PCI audit, or complete a Self-assessment Questionnaire (SAQ) to validate compliance. In addition to this, you will have to present the results of the quarterly network perimeter scans (which had to be performed by an approved scanning vendor), evidence of internal vulnerability scans, and evidence of application and network penetration tests. In other words, you have to prove to the card brands that your company practices sound patch management and vulnerability management processes.

Table 3.5 Compliance Validation for Merchants

Level	American Express	MasterCard	Visa USA
Level 1	Annual on-site review by QSA (or internal auditor if signed by officer of merchant company) Quarterly scan by ASV	Annual on-site review by QSA Quarterly scan by ASV	Annual on-site review by QSA (or internal auditor if signed by officer of merchant company) Quarterly scan by ASV
Level 2	Quarterly scan by ASV	Annual Self-assessment Questionnaire Quarterly scan by ASV	Annual SAQ Quarterly scan by ASV
Level 3	Quarterly scan by ASV (recommended)	Annual SAQ Quarterly scan by ASV	Annual SAQ Quarterly scan by ASV
Level 4	N/A	Annual SAQ (recommended) Quarterly scan by ASV (recommended)	Annual SAQ (recommended) Quarterly scan by ASV (recommended)

NOTE

Discover and JCB handle merchant PCI compliance validation differently. Contact the payment brand for more information.

NOTE

Although American Express and Visa allow Level 1 merchants to have their PCI compliance validated by the merchant's internal audit group, MasterCard does not explicitly allow this. If this affects your company, contact MasterCard for clarification.

Table 3.6 Compliance Validation for Service Providers

Level	American Express	MasterCard	Visa USA
Level 1	Annual on-site review by QSA (or internal auditor if signed by officer of service provider company) Quarterly scan by ASV	Annual on-site review by QSA Quarterly scan by ASV	Annual on-site review by QSA Quarterly scan by ASV
Level 2	N/A	Annual onsite review by QSA Quarterly scan by ASV	Annual on-site review by QSA Quarterly scan by ASV
Level 3	N/A	Annual SAQ Quarterly scan by ASV	Annual SAQ Quarterly scan by ASV

NOTE

Discover and JCB handle service provider PCI compliance validation differently. Contact the payment brand for more information.

For the penetration tests, you will need to test every external application that stores, processes, or transmits cardholder data, and test the external network segment, also known as the demilitarized zone (DMZ). Penetration tests are not vulnerability scans. They are much more involved, and are not automated. You cannot simply buy a tool and execute a command to run such tests. While PCI does not require penetration tests to be performed by a third party, the authors of this book recommend that you do, unless you have strong ethical hacking expertise in-house.

When submitting a SAQ, it will have to be signed by an officer of your company. At the present time, there is no court precedent for liability; however, industry speculation is that this person may be held accountable in a civil court, especially if he or she commits an act of perjury.

WARNING

At the time of publication, the SAQ has not been updated to reflect the changes from PCI DSS 1.0 to 1.1.

If you are planning on submitting a Report On Compliance (ROC) instead of the SAQ, you will need to follow the document template outlined in the PCI DSS Security Audit Procedures document. After the SAQ has been filled out or the ROC has been completed, it must be sent along with all of the necessary evidence and validation documentation to either the acquirer, the business partner, or to the card brand directly. It depends on who requested the compliance validation in the first place.

Roots of PCI

PCI DSS is the standard that has evolved from the efforts of several card brands. In the 1990's, the card brands developed various standards to improve the security of sensitive information. In the case of Visa, different regions came up with different standards (i.e., European countries were subject to different standards than the US). In June 2001, Visa USA launched the Cardholder Information Security Program (CISP). The CISP Security Audit Procedures document version 1.0 was the grand-daddy of PCI DSS. These audit procedures went through several iterations, and made it to version 2.3 in March of 2004. At this time, Visa was already collaborating with MasterCard. Their agreement was that merchants and service providers would undergo annual compliance validation according to Visa's CISP Security Audit Procedures, and would follow MasterCard's rules for vulnerability scanning. Visa maintained the list of approved assessors and MasterCard maintained the list of approved scanning vendors.

This collaborative relationship had a number of problems. The lists of approved vendors were not well-maintained, and there was no clear way for security vendors to get added to the list. Also, the program was not endorsed by all card brand divisions. Other brands such as Discover, American Express, and JCB were running their own programs. The merchants and service providers in many cases had to undergo several audits just to prove compliance to each brand, which was clearly costing too much. For that and many other reasons, all card brands came together and created the PCI DSS 1.0, which gave us the concept of PCI compliance.

Unfortunately, the issue of ownership still was not addressed, and a year later the PCI Security Standards Council was founded (https://www.pcisecuritystandards.org). Comprised of American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International, PCI Co (as it came to be known) maintains the ownership of the DSS, most of the approved vendor lists, training programs, and so forth. There are still exceptions, as the list of approved payment application assessors at the time of this book's publication is still maintained by Visa.

Each card brand/region maintains its own security program beyond PCI. These programs go beyond the data protection charter of PCI and include activities such as fraud prevention. The information on such programs can be found in Table 3.5. In certain cases, PCI ROC needs to be submitted to each card brand's program office separately.

Table 3.7 Brand Security Programs

Card Brand	Additional Program Information
American Express	Web: www.americanexpress.com/datasecurity E-mail: American.Express.Data.Security@aexp.com
Discover	Web: www.discovernetwork.com/resources/data/data_security.html E-mail: askdatasecurity@discoverfinancial.com
JCB	Web: www.jcb-global.com/english/pci/index.html E-mail: riskmanagement@jcbati.com
MasterCard	Web: www.mastercard.com/sdp E-mail: sdp@mastercard.com
Visa USA	Web: www.visa.com/cisp E-mail: cisp@visa.com
Visa Canada	Web: www.visa.ca/ais

More about PCI Co

PCI Co's charter provides oversight to the development of PCI security standards on a global basis. It formalizes many processes that existed informally within the card brands. PCI Co published the updated DSS, now at version 1.1, which is accepted by all brands and international regions, and it refreshed most of the supporting documentation.

PCI Co is technically an independent industry standards body, and its exact organizational chart is published on its Web site. Yet it remains a relatively small organization, primarily comprised of the employees of the brand members. In fact, the role of answering e-mails sent to info@pcisecuritystandards.org rotates every month among the representatives of the card brands.

The industry immediately felt the positive impact of PCI Co. The merchants and service providers can now play a more active role in the compliance program and the evolution of the standard, while the Qualified Security Assessor Companies (QSACs) and Approved Scanning Vendors find it much easier to train their personnel.

Approved Assessor and Scanner Companies

PCI Co now controls what companies are allowed to conduct on-site DSS compliance audits. These companies, known as Qualified Security Assessor Companies (QSACs), have gone through the application and qualification process, having had to demonstrate compliance with tough business, capability, and administrative requirements. QSACs also had to invest in personnel training and certification to build up a team of Qualified Security Assessors (QSAs).

NOTE

QSACs are only permitted to conduct on-site DSS audits. They are not automatically granted the right to perform perimeter vulnerability scans.

QSACs have to recertify annually, and have to re-train their internal personnel. The exact qualification process and the requirements are outlined on PCI Co's Web site, so we will not go into it in detail; however, of particular interest are the insurance requirements. QSACs are required to carry high coverage policies, much higher than typical policies for the professional services firms, which becomes important later.

NOTE

QSACs are approved to provide services in particular markets: USA, Asia Pacific, CEMEA (Central Europe, Middle East, and Africa), Latin America and the Caribbean, and Canada. The qualification to service a particular market

depends on QSAC's capabilities, geographic footprint, and payment of appropriate fees.

To become an Approved Scanning Vendor (ASV), companies must undergo a process similar to QSAC qualification. The difference is that in the case of QSACs, the individual assessors attend classroom training on an annual basis, whereas ASVs submit a scan conducted against a test Web perimeter. An organization can choose to become both QSAC and ASV, which allows the merchants and service providers to select a single vendor for PCI compliance validation.

Qualified Security Assessors

QSA is a certification established by PCI Co. Individuals desiring this certification must first and foremost work for a QSAC or for a company in the process of applying to become a QSAC. Then, they must attend official training administered by PCI Co, and pass the test. They must also undergo annual requalification training to maintain their status. An individual may not be a QSA unless he or she is presently employed by a QSAC.

WARNING

Only QSAs in good standing and employed by a QSAC are permitted to perform on-site PCI audits.

Overview of PCI Requirements

PCI DSS version 1.1 is comprised of six control objectives that contain one or more requirements:

- Build and Maintain a Secure Network
  - Requirement 1: Install and maintain a firewall configuration to protect cardholder data
  - Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

- Protect Cardholder Data
  - Requirement 3: Protect stored cardholder data
  - Requirement 4: Encrypt transmission of cardholder data across open, public networks
- Maintain a Vulnerability Management Program
  - Requirement 5: Use and regularly update anti-virus software
  - Requirement 6: Develop and maintain secure systems and applications
- Implement Strong Access Control Measures
  - Requirement 7: Restrict access to cardholder data by business need-to-know
  - Requirement 8: Assign a unique ID to each person with computer access
  - Requirement 9: Restrict physical access to cardholder data
- Regularly Monitor and Test Networks
  - Requirement 10: Track and monitor all access to network resources and cardholder data
  - Requirement 11: Regularly test security systems and processes
- Maintain an Information Security Policy
  - Requirement 12: Maintain a policy that addresses information security

As you can see, these 12 requirements cover the whole spectrum of information technology (IT) areas. Some requirements are very technical in nature (e.g., Requirement 1 calls for specific settings on the firewalls), and some are process oriented (e.g., Requirement 12).

PCI is the most tactical regulation, which has a significant benefit. It makes things easier for both the companies that have to comply with the standard, and the auditors. For example, when compared to the Sarbanes Oxley Act of 2002 (SOX), companies do not have to invent or pay for controls; they are already provided. Also, PCI is much less nebulous than the Health Insurance Portability and Accountability Act (HIPAA) Security Rule with its "required" and "addressable" requirements.

PCI compliance validation may affect more than what you consider the "cardholder environment." According to PCI DSS 1.1, the scope can include the cardholder data environment only if adequate network segmentation is in place. In most

cases, this implies the use of dedicated firewalls and non-routable virtual local area networks (VLANs). If you do not have such controls in place, the scope of PCI compliance validation will cover your entire network. Think about it: if you cannot ensure that your cardholder data is confined to a particular area, then you cannot focus on this area alone, and you have to look everywhere.

Point of sale (POS) systems also may change the scope of compliance validation. If POS system does not have any connections to the rest of the merchant's network, it may be excluded from the validation process. The compliance of the POS system itself is determined by a Qualified Payment Application Security Company (QPASC) or the card brands. Contact the card brands to determine of your POS system has already been determined to be compliant.

NOTE

Just because a POS system is on the list of compliant payment applications, does not mean that your particular implementation is compliant. You should work with the application vendor to verify this.

If wireless technology is used within the cardholder data environment, or if the cardholder data environment is not adequately segmented, separate procedures will have to be used to validate compliance. PCI Co does not consider wireless technologies to be sufficiently mature; therefore, they are treated with extra caution.

For the benefit of consumers that may be more familiar with a brand name than a parent company, PCI compliance is validated for every brand name. Thus if a company has several divisions or "doing business as" (DBA) names, each entity has to be validated separately. For reporting simplicity, the ROCs and SAQs may note that they include validation of multiple brand names.

You may discover that sometimes it is necessary to bend the rules for a legitimate business need. For example, you may need to temporarily store cardholder data unencrypted for troubleshooting purposes. As long as you follow reasonable precautions, card brands understand this need. Another example may include recording certain call center conversations for customer service purposes. Again, card brands understand that these recordings may contain cardholder data, so accommodations are made accordingly.

In many cases, compensating controls have to be used to achieve compliance when your company cannot meet a given requirement exactly. The important thing to remember about compensating controls is that they have to go beyond the requirements of PCI to provide the same or higher assurance of cardholder data protection. When compensating controls are claimed, additional documentation must be completed. The Compensating Control Worksheet, which can be found in Appendix C of the PCI DSS Security Audit Procedures document, must be filled out for each situation.

Risks and Consequences

If you are a Chief Financial Officer (CFO) or a comptroller, you are probably asking the question: "Why would I need to spend the money on PCI?" Good question—there are fines! Unfortunately, the fine schedules are not well defined. Your company's contract with the acquiring bank probably has a clause in it that any fines from the card brand will be "passed through" to you. With all compliance deadlines passed, the fines could start tomorrow. Visa USA has announced that it will start fining acquirers (which will pass on the costs to the merchant) between $5,000 and $25,000 per month if their Level 1 merchants have not demonstrated compliance by September 30, 2007, and Level 2 merchants have not demonstrated compliance by December 31, 2007. In addition, the fines of $10,000 per month may already be assessed today for prohibited data storage by Level 1 or Level 2 merchant (http://usa.visa.com/about_visa/press_resources/news/press_releases/nr367.html).

What is certain is that you will be fined up to $500,000 if non-compliant and compromised. Believe it or not, if compromised, this will be the least of your concerns. Civil liabilities will dwarf the fines from the card brands. Some estimates place the cost of compromise at $80 per account. Some companies that have been compromised have been forced to close their doors. According to PCI Co and the Ponemon Institute study, the per capita cost of a data breach has gone up more than 30 percent in the past year.

In addition to fines, after a compromise, assuming you are still in business, the company automatically gets Level 1 status for compliance verification and the audit process gets significantly more expensive. Consider the cost of data forensic services, increased frequency of reporting, and so forth. Not to mention that you will still have to comply with PCI eventually if you want to continue to be able to accept them, or be in the related line of business.

Let's use TJX company, which operates stores like TJ Maxx, Marshalls, and so forth, as a case study. On January 17, 2007, TJX announced that they were compromised. Because they did not have robust monitoring capabilities such as those mandated by PCI, it took them a very long time to discover the compromise. The first breach actually occurred in July 2005. TJX also announced that 45.7 million credit card numbers were compromised. Conservative estimates put a five-year cost estimate to TJX at over one billion dollars. To date, over 20 separate law suits have already been filed against TJX.

Whether you believe your company to be the target or not, the fact is that if you have cardholder data, you are a target. Cardholder data is a valuable commodity that is traded and sold illegally. Organized crime units profit greatly from credit card fraud, so your company is definitely on their list. International, federal and state law enforcement agencies are working hard to bring perpetrators to justice and shut down the infrastructure used to aid in credit card related crimes; however, multiple forum sites, Internet chat channels, and news groups still exist where the buyers can meet the sellers. Data breaches like the one at TJX are not the work of simple hackers looking for glory. Well-run organizations from the Eastern European block and select Asian countries sponsor such activity.

Privacyrights.org maintains the history of the compromises and impacts. Since 2005, over 150 million personal records have been compromised. This includes companies of all sizes and lines of business. If the industry does not get this trend under control, the US Congress will give it a try. In February 2007, Congress has already debated a data retention bill. It is a safe bet that any legislation that is enacted into law will carry much stiffer penalties than the card brands assess today.

Today, according to the information security experts, the following constitute the greatest risk of a data breach:

- Wireless networks
- Lack of adequate network segmentation
- Application remote exploit
- Compromise by an employee with access

Last, but not least is the involvement by the Federal Trade Commission (FTC). Sometimes protection of credit card data also falls within the realm of the Gramm-Leach-Bliley Act (GLBA), a law that protects the consumers' right to privacy. Disclosure of the credit card information can lead to identity theft. Remember the

ChoicePoint incident? That company was fined $10 million by the FTC, and had to reimburse expenses to the victims of the identity theft.

Benefits of Compliance

One of benefits of PCI compliance is that your organization will not be fined in case of a compromise. If the post-mortem analysis shows that your company was still compliant at the time of the incident, no fines will be assessed, and you will be granted what is known as "safe harbor." It is likely that your company will be taken to civil court regardless of your compliance status should a breach occur. However, a jury will be much more sympathetic to your company's case if you can show that due diligence was practice by the virtue of PCI compliance.

More immediately, if your company is a Level 1 or Level 2 merchant, you may be eligible to receive a part of the $20 million in financial incentives from Visa. In December 2006, Visa USA announced their PCI Compliance Acceleration Program (CAP). Those merchants that demonstrate compliance by August 31, 2007, may receive a one-time payment incentive. The press release for this program can be found at http://usa.visa.com/about_visa/press_resources/news/press_releases/nr367.html.

Another form of incentive deals with transaction costs. As part of the CAP program, Visa USA announced that the interchange rates will not be discounted for acquirers that have not validated PCI compliance of their merchant clients. Come October 1, 2007, acquirers may start passing the increased costs to the merchants that have not reached compliance.

Whether it is avoiding fines or getting incentives, the greatest benefit of PCI compliance is the peace of mind that your IT infrastructure and business processes are secure. Again, if you are a CFO or a comptroller, think about the data breach cost avoidance. Crunch the ROI numbers as you read more and more about TJX's plight.

Your marketing department may also appreciate the compliance status. The name of your company will be listed on each card brand's Web site. You can also get certification logos from your QSAC, a must have for your Web site. A recent poll showed that 40 percent of consumers will not deal with a company they know has been breached, so by addressing your customers' concerns you may get more business in the process.

Summary

PCI refers to the DSS established by the credit card brands. Any company that stores, processes, or transmits cardholder data has to comply with this data protection standard. Effectively, all of the target compliance dates have already passed, so if your company has not validated compliance you may be at risk of fines. PCI is composed of 12 requirements that cover a wide array of business areas. All companies, regardless of their respective level, have to comply with the entire standard as it is written. The actual mechanism for compliance validation varies based on the company classification. The cost of dealing with data breaches keeps rising, as does their number. Companies that do not take compliance efforts seriously may soon find themselves out of business. Yet the companies that are proactive about compliance may be able to capture additional business from the security-conscious consumers.

Solutions Fast Track

PCI

- ☑ PCI is used synonymously with PCI DSS.
- ☑ If you are not compliant already, you are late. Most compliance deadlines have already passed.
- ☑ PCI is not perfect, so be prepared for bumps in the road.
- ☑ PCI compliance cannot be a project—it is a process. Keep your project on a more manageable level, perhaps one for each DSS requirement.

Get an Advice From Someone Who Knows

- ☑ Seek the help of a trusted advisor who can help steer your compliance efforts.
- ☑ PCI DSS requirements are often misinterpreted. Validate what you believe to be true or what you are being told.
- ☑ When selecting a trusted advisor, look for the reputation and stability before you look at cost. The two of you might have to team up in the courtroom, so build a relationship.

Get the Facts

- ☑ Get an assessment by a QSAC. If your company is close to being compliant, it will take very little additional effort to turn an assessment report in to a ROC.
- ☑ Contract the services of the ASV for performing the quarterly perimeter scans and penetration tests.
- ☑ Consider using the same company for both assessments and scans. That way you have better communication.
- ☑ Deal directly with a QSAC, not with a middle man.

Start at the Top

- ☑ Get an endorsement from the company's senior management and business stakeholders.
- ☑ Start your remediation efforts with higher level concepts: first the policy, then the process, then standards and procedures.
- ☑ Don't forget to document everything!

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to **www.syngress.com/solutions** and click on the **"Ask the Author"** form.

Q: Where do I start with my compliance efforts?

A: If your organization is a merchant, your acquirer's account manager can help lay out a plan. If your organization is a service provider, then your business partner should help clarify your obligation.

Q: I'm getting conflicting information about PCI compliance validation. What do I do?

A: Always refer back to the legal contracts you have in place with the party that requires you to be compliant. Your legal council should be able to clarify these requirements.

Q: Compliance costs too much. Is it worth it?

A: Yes, when you consider the cost of fines, civil liabilities, government fines, and so forth.

Chapter 4

Building & Maintaining a Secure Network

Solutions in this chapter:

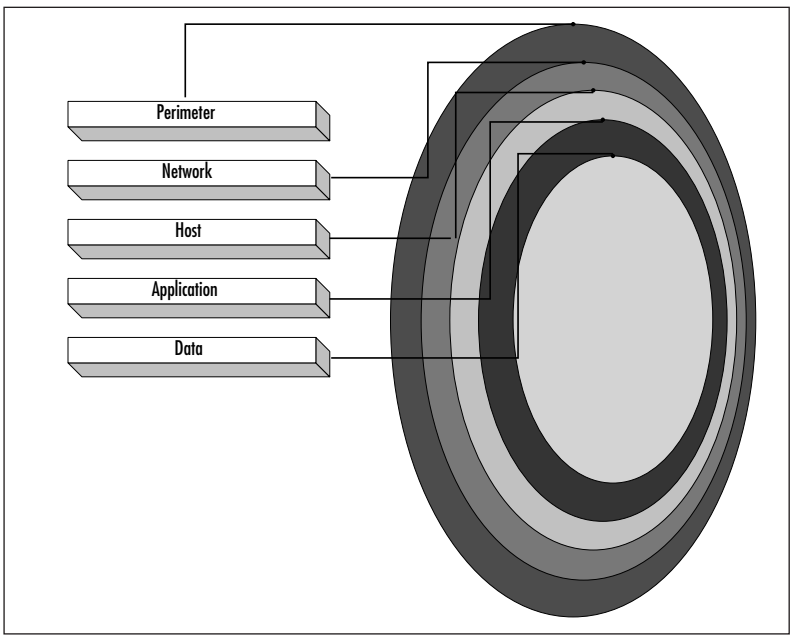
- **Installing and Maintaining a Firewall Configuration to Protect Cardholder Data**
- **Choosing an Intrusion Detection or Intrusion Prevention System**
- **Installing Appropriate Antivirus Software**
- **Changing Vendor-supplied Defaults for Systems Passwords and Other Security Parameters**
- **Performing Internal and External Vulnerability Assessments**

- ☑ **Summary**
- ☑ **Solutions Fast Track**
- ☑ **Frequently Asked Questions**

Introduction

When thinking about securing a network, it is best to think of it in terms of defense-in-depth or a layered security approach. It would be great if we could rely on one type of technology or a single device to provide all of our security, but that's not realistic. Some professionals use the analogy that security is like an onion—it has layers. Each layer doesn't stand alone, but together they're tough and solid. A firewall is one layer, but not necessarily the first layer. Figure 4.1 shows the different layers. The packet-filtering router that actually connects your company to the Internet is the first layer. Configure a small rule set to filter out basic unwanted traffic like Internet Control Message Protocol (ICMP), finger, and anything else that you can live without ever crossing into your network space. The next layer is the devices that make up your internal network infrastructure. Firewalls, intrusion detection systems (IDses), and switches all contribute to this layer of security. Layer three is the host-based security that you might have installed on each host. Host-based intrusion detection, antivirus software, and so forth would cover this layer to include the hardening of the operating system itself. The fourth layer covers the application itself. Any hardening of the application, access controls, and file/library permissions fall into this layer. The final layer covers protecting the data itself. Encrypting the data stored on the system is one of the easiest ways to protect it.

Figure 4.1 Layered Security: Defense in Depth



Installing and Maintaining a Firewall Configuration

Why do we need a firewall? Besides the obvious, the Payment Card Industry (PCI) standard requires it; we need to reduce our risk by protecting our systems and networks from attempts to exploit known and unknown vulnerabilities. That all sounds fine for a formal response, but what are we really doing? We're adding privacy to the internal network by restricting access to the systems on our internal network. A firewall is simply a noise filter or device that controls unwanted traffic into a company's network from outside, and can play an important role by segregating sensitive areas from the rest of the company's internal network.

Let's take a look at firewall placement and configurations. Remember, this book isn't meant to be an authority on firewalls, but it will give you some ideas. From time to time I'll refer back to the PCI Self-assessment Questionnaire (SAQ) and/or the Security Audit Procedures to clarify.

Firewall Overview

There are literally dozens of firewall manufacturers in the world, but only a few different types of firewalls. The PCI standard does not specify what brand of firewall to use, but it does state what it needs to provide in order to provide the level of security required for your environment. It needs to be robust enough to allow the appropriate amount of configurations to be applied. The differences in firewalls is in the way they handle the packets of data for acceptance or rejection. Only if the packet meets a certain predetermined criteria is it allowed to pass through the firewall. This helps to reduce the traffic flow into the network. Firewalls can also be used internally. Most people think a firewall is only used for connectivity to the Internet or non-private networks. Although the perimeter is the primary consideration when implementing a firewall solution, it can also be used on the private network to protect more sensitive networks or systems from traffic on the private network. The three types of firewalls we will discuss are *packet filtering*, *proxies* and *stateful* packet inspection firewalls.

Packet-filtering Firewalls

Packet filters work a little differently than a proxy. They still inspect packets, but they do it at the network layer (Layer 3) of the Open Systems Interconnection (OSI) model. This is where the routing of packets takes place. A packet-filtering firewall

allows or denies packets based on the Internet Protocol (IP) address, protocol, and source and destination port numbers being used. A router is essentially a packet filter. Most routers are fast and efficient and the technology is widely available, but they are limited in what information in a packet they can analyze. The syntax of the rule set is sometimes hard to remember, and there is always the occasional bug and vulnerability discovered in these simple devices. Table 4.1 lists some of the pros and cons of packet filtering firewalls.

Table 4.1 Packet Filter Pros and Cons

Pros	Cons
Low cost	Rules are sometimes hard to configure
Fast and efficient	Router performance affected
Technology is widely available	Bugs and vulnerabilities are more prone in this technology

NOTE

Most routers have a specific job, routing information to and from your network in the most efficient manner possible. Making the rule set too complex and lengthy will ultimately affect the performance of your router. They should be configured to only filter out basic unwanted traffic, leaving the brunt of the work up to a real firewall.

Proxy Firewalls

Proxy firewalls work by making every connection requested across the firewall on behalf of the client. Packets are scrutinized at the application layer of the OSI seven-layer model, and are examined for their compliance with specific rules and then either permitted or denied.

OSI Review

The OSI model has seven layers:

- **Physical** The physical layer establishes the communications medium for the network (i.e., cabling, voltage, hubs, repeaters).
- **Data Link** The data link layer provides functional and procedural instructions to transfer data between networked components (i.e., Ethernet, ATM, Frame Relay).
- **Network** The network layer provides network routing functions to connect networks that make up the Internet.
- **Transport** The transfer layer simply transfers data between the end users and provides reliability and error control (i.e., Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).
- **Session** The session layer controls the connections between remote and local applications. The management and termination of sessions (i.e., checkpointing, adjournment, termination, and restart procedures).
- **Presentation** The presentation layer transforms the data for the application layer to provide a standard interface (i.e., American Standard Code for Information Interchange (ASCII)-coded files, data encryption, Multipurpose Internet Mail Extensions [MIME]).
- **Application** The application layer directly serves the end user by performing common application services for application processes. This is how real work gets done. (i.e., file transfer, database access).

Proxy firewalls are much slower than packet-filtering firewalls, but are considered to be a more secure solution offering a higher level of security. They are suitable for certain types of organizations that may be more security conscious like financial institutions and government organizations, but have a significant impact on network performance. Table 4.2 describes the pros and cons of why a proxy may not be the best solution for a company dealing with PCI data.

Table 4.2 Proxy Pros and Cons

Pros	Cons
"Intelligent" filtering	May require modification of servers/clients
Includes user-level authentication	Much slower than packet filtering
Normally provides good logging	Extensive configurations and management

WARNING

Remember, proxies are better used to monitor or control outbound traffic. That's not to say they can't be used for inbound traffic, but think about what you're trying to accomplish here, a balance between security and performance. There's a possibility that you could be processing thousands of transactions an hour depending on the size of your company. A proxy may not be the best firewall solution where speed is important.

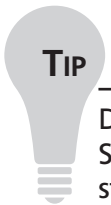
Stateful Inspection Firewalls

Stateful inspection firewalls combine the speed of packet filters with the control of proxy firewalls. They have the ability to filter packets at the network layer, and then determine if session packets are valid and evaluate the contents of the packets at the application layer. Stateful inspection firewalls allow for direct connections between clients and hosts.

Stateful inspection firewalls offer strong security along with good performance and transparency to end users, unlike the packet filtering and proxy firewalls. Algorithms are used to recognize and process application layer data instead of having to run an application specific proxy. They keep track of the "state" of a connection and, in most cases, examine each packet to see if it is part of an authorized connection. Since the UDP protocol has no "state," UDP return packets arriving within a prescribed time window are allowed in. This technology is expensive and, due to the complexities of the configuration, have the added risk of being misconfigured thus adding additional risk to you environment. Table 4.3 shows the pros and cons of the stateful packet inspection firewall's balance of speed and security, which is a better solution for companies working with PCI data.

Table 4.3 Stateful Packet Inspection Pros and Cons

Pros	Cons
Fast	Expensive
Transparent to the user	Complex configurations
Multiple inspection points at different layers of the OSI	UDP is stateless and requires additional configurations



TIP

Don't get too hung up on firewall types. Section 1.3.3 of PCI Data Security Standard (DSS), DSS version 1.1 is establishing a requirement that only a stateful inspection firewall (dynamic packet filtering) should be used. Therefore, this decision has already been made.

Firewall Architectures

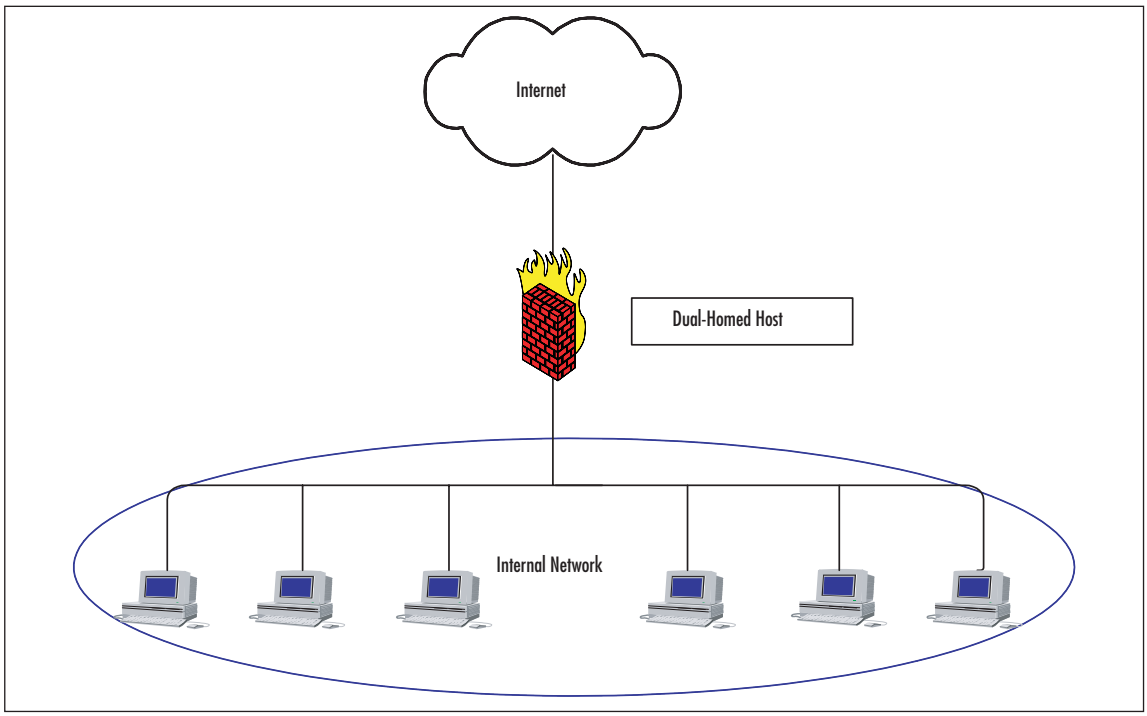
Firewall architectures vary in complexity, from the easy-to-set-up screening router (which is not discussed here), to a dual in-line firewall configuration. A screening router, a router with only a few rule sets configured, is an unacceptable solution; therefore, it can be ruled out. The three more common types of architectures that we'll discuss are the *dual-homed host*, *screened host*, and the *screened subnet*. We also talk about architectures that have in-line firewall configurations and the benefits of such a design.

Dual-Homed Host

The dual-homed host architecture deploys a single machine connected to two networks and acts as a gateway. This configuration is better suited for a proxy firewall in which all traffic and transactions go through this host before proceeding on to another network. This is a relatively simple configuration and offers added security that having only a screening router does not. As mentioned earlier, proxy firewalls require a lot of configuration, and without configuring packet forwarding traffic will not pass. Therefore, each traffic type needs to be analyzed and the firewall configured to allow the traffic or it's denied. Figure 4.2 shows a simple description of the placement of a dual-homed host between the Internet and your private network. It

sounds simple, but the complexities in the configuration may make it infeasible when considering the appropriate level of security for your PCI environment.

Figure 4.2 Dual-homed Host



NOTE

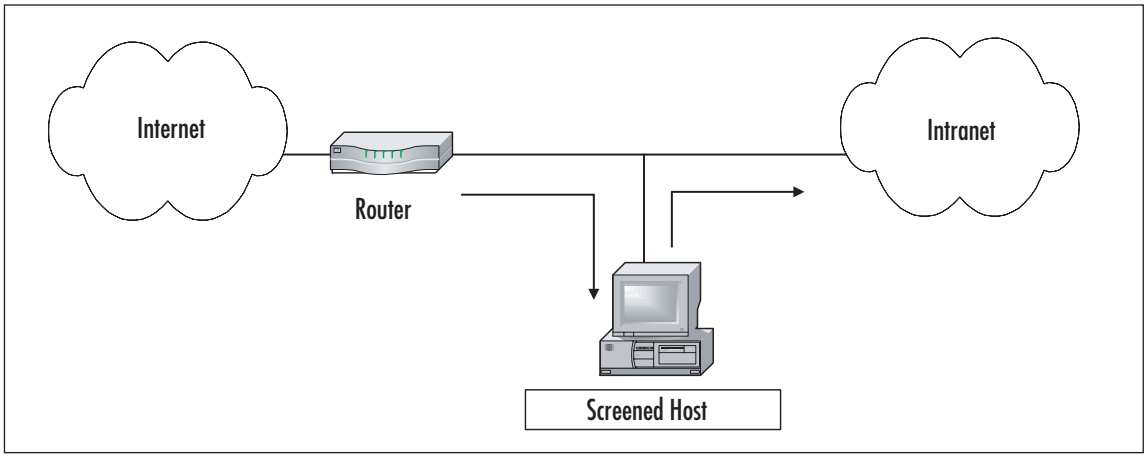
You will see a dual-homed host in the configuration sometimes called a Bastion Host. In IT, a bastion host is usually the only computer a company will allow to be touched by the public network, and its design is so that it screens the rest of the internal network from outside elements. In medieval times, a bastion was a fortification that projected outward from the main part of a castle and offered an advantage point against adversaries.

Screened Host

Screened host configurations offer a little more complexity to your architecture. As you'll notice on Figure 4.3, a router is introduced into the environment and provides screening at the perimeter of the network. External users are still able to get to the

screened host, and traffic still flows through the host acting as a gateway or proxy into and out of the network for added security. You should be starting to understand the layering approach at this point. Instead of a single device providing all of the security, the router is filtering out unwanted traffic and the screened host is adding additional security by inspecting all of the traffic and allowing or disallowing traffic as defined in the security policy.

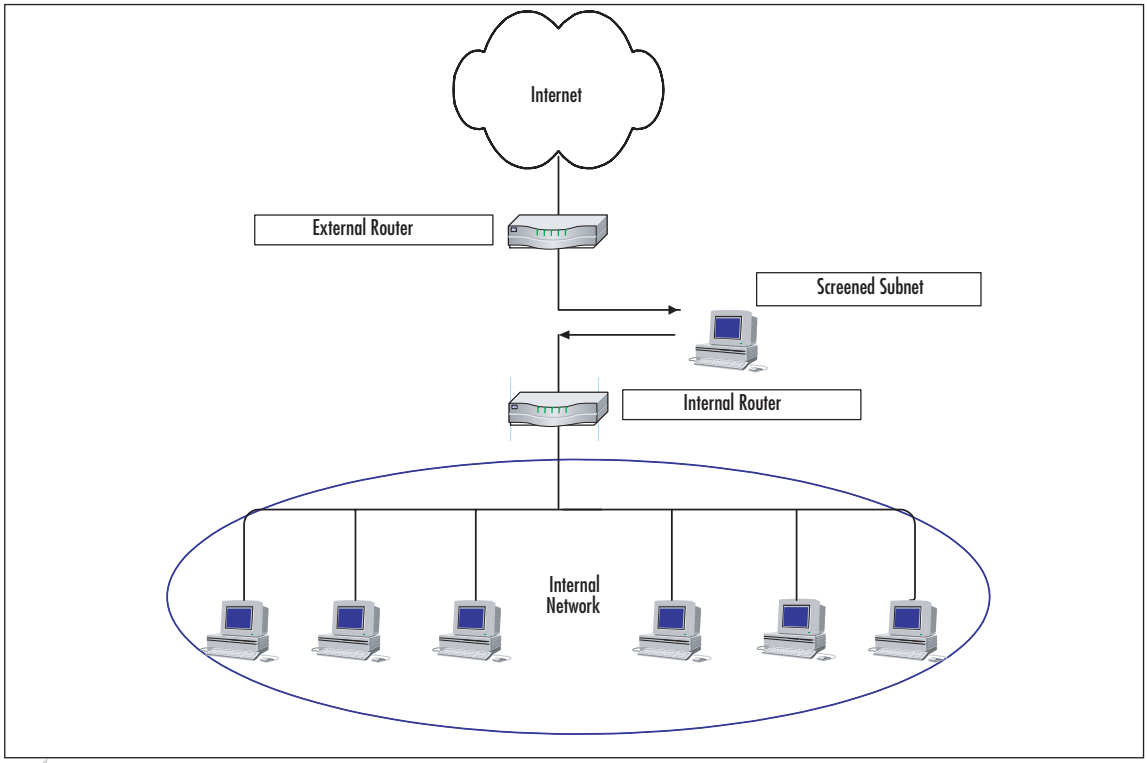
Figure 4.3 Screened Host



Screened Subnet

The screened subnet configuration is a combination of the dual-homed host and screened host architectures. The screening router is still the first line of defense into the corporate network, and filters incoming traffic between the Internet and the publicly accessible hosts. As shown in Figure 4.4, the host could be a dedicated server or have several services running and could also be a firewall (with several DMZs configured for separation) where all connections to and from the internal network are made. Notice the additional layer of security by putting another router in place to further restrict access into the private network.

Figure 4.4 Screened Subnet



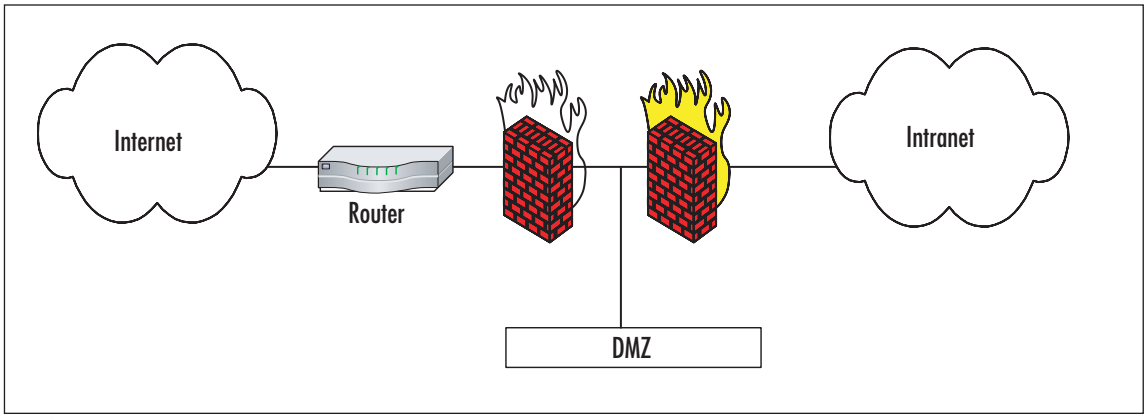
NOTE

In this particular configuration, it is not unusual to see the second router replaced with a firewall's screened hosts sitting off of one of several physical DMZ ports, which most firewalls offer today.

Dual Firewall Configuration

A dual firewall configuration is the optimal network configuration. There are multiple layers of security in this configuration. The router still provides the first layer of security, and the first firewall provides stateful inspection of traffic to the DMZ(s). The second firewall prevents any traffic originating from the Internet or DMZ(s) to access the corporate network, as shown in Figure 4.5. It is recommended to have disparate firewalls for this configuration in the event one firewall is compromised. The odd of breaching both firewalls is fairly large.

Figure 4.5 Dual Firewall Configuration



NOTE

If you decide to implement a dual firewall configuration, consider multiple vendors for your design, keeping in mind that if a single vendor is chosen, the vulnerabilities will exist for both.

PCI DSS Requirements

Section 1.1 of the PCI DSS guides you through the process of configuring and maintaining your firewall. There is no real science to deciding on what type of firewall and configuration to use, just some forethought. PCI requirements make is easy for you. The DSS tells you what type of firewall you can use, how it must be configured, how to maintain it, and what to protect against.

Establish Firewall Configuration Standards

The DSS doesn't waste any time getting into change management. Section 1.1.1 requires a formal process for approving and testing all external network connections and changes to the firewall configuration. There are a couple of things going on here. First, all external connections have to be approved and tested. Approval implies that management must know and agree to the connection. Once the connection is made, it must be tested. This is usually done by penetration testing. Penetration testing is the authorized testing of security controls at the perimeter (connection). Your organization may prefer to call it a vulnerability assessment or external risk assessment, but

generally we are talking about the same thing. Lastly, the firewall should be baselined and any changes to the configuration thereafter must be approved. Each of the stakeholders should have a say in whether or not the changes actually get implemented.

It's much easier to understand what needs to be secured if you can see it on paper. Section 1.1.2 shows a current network diagram. All connections to the cardholder data should be clearly documented including any wireless networks. The network diagram includes all external connections to the Internet and all network devices, systems, and dataflows. This diagram needs to remain current at all times. With a good change management process, keeping the network diagram up-to-date is a simple task.

Dataflow are often forgotten when putting together an accurate diagram. These are the directional arrows that show the flow of data. Additionally, the type of data and the protocol needs to be a consideration to meet requirements 1.1.6 and 1.1.7. Requirement 1.1.6 requires justification and documentation for any available protocols besides Hypertext Transfer Protocol (HTTP), Secure Socket Layer (SSL), Secure Shell (SSH), and Virtual Private Networks (VPN). Requirement 1.1.7 also requires justification of the use of risky protocols such as File Transfer Protocol (FTP) and Telnet. In order to document dataflows accurately, a list of services and ports necessary to do business needs to be identified. This list should also meet the requirement of section 1.1.5. Section 1.1.4 may also be of use here. The administrator needs accurate documentation of all groups, roles, and responsibilities for logical management of network components. This is especially helpful to administrators when implementing the rule sets.

Now that you have all of your Internet connections documented and your network clearly defined, firewalls need to be implemented at each connection point and between any DMZ and the internal network. Depending on how robust the firewall solution is, it may have DMZs built in. If not, the dual firewall solution would need to be implemented in order to comply with 1.1.3 of the DSS. It requires a firewall between DMZs and the internal network. It sounds trivial, but interpretation is everything. There isn't a lot of information regarding the router configurations. Requirement 1.1.9 states that router configuration standards must exist. There aren't a lot of details for 1.1.9, but if you follow the same steps that the DSS requires for the firewall configurations and apply it to the routers, you should not have any problems meeting this requirement. Lastly, 1.1.8 requires quarterly reviews of the firewall and router rule sets for accuracy.

Build Secure Firewall Configurations

Sections 1.2, 1.3, 1.4, and 1.5 can be rolled into building secure firewall configurations. The requirements are interrelated and thus can be discussed at the same time. Section 1.2 focuses on denying traffic from untrusted networks and hosts. Section 1.3 restricts access to any system storing cardholder information from any publicly accessible system in the DMZ. Section 1.4 prohibits access to systems that house cardholder information from the Internet. Finally, Section 1.5 requires IP masquerading. Let's take a look.

Denying Traffic from Untrusted Networks and Hosts

Confidentiality, integrity, and availability are at the heart of Section 1.2. This firewall configuration has to accomplish several things. The rule of thumb here is to deny most traffic. The few types of traffic allowed should only be what is absolutely necessary to conduct business. It is much easier to filter everything initially than to only open the required ports and allow specific types of protocols to traverse those ports. This is where a good network diagram with dataflows, coupled with an accurate list of required services, ports, and protocols, is worth its weight in gold.

Denying all traffic from "untrusted" networks and hosts is easy to accomplish. Many firewall solutions do this right out of the box. If not, there is usually a rule that can be configured to do this. It all boils down to "deny all." Don't be confused here. Denying all doesn't necessarily deny "all" traffic through the firewall. It usually only denies incoming traffic, not outgoing. In order to deny outgoing traffic, a rule would need to be applied to the rule set for outbound traffic.

With the traffic being denied for all inbound traffic, specific rules need to be applied that allow for a few necessary protocols that are already acceptable based on the DSS. Rules to allow HTTP, SSL, SSH and VPN traffic should be implemented. Just because they are allowed doesn't mean you should allow these protocols by default. Verify the business need against your list of ports, protocols, and services first. To add even more security, if the source of traffic can be narrowed down to specific networks or hosts, apply a rule only allowing such.

Restricting Connections

Section 1.3 in the DSS gets pretty granular with restricting connections between publicly accessible servers and any system component that stores cardholder data. What does this mean to you? The database cannot be in a DMZ that is publicly accessible. Stateful inspection firewalls must be used. Inbound and outbound traffic is

restricted to only that which is needed to conduct business and is documented. If traffic is not explicitly allowed in the rule set, it should be denied. Any Request For Comment (RFC) 1918 addresses are not allowed from the Internet. Personal firewalls are implemented on mobile units. And lastly, the routers comply with the established change management rules.

RFC 1918 Explained

RFC 1918 focuses on two major challenges with the Internet. One is the concern within the Internet community that all the globally unique address space (routable IP addresses) will be exhausted. Additionally, routing overhead could grow beyond the capabilities of the Internet Service Providers (ISPs). The term "Private Network" is a network that uses the RFC 1918 IP address space. Internal networks (private) can allocate addresses from this address space in order to provide communication capabilities for devices on the network. This alleviates the need for assigning a globally routable IP address for every computer, printer, and other device that an organization uses. It also reduces the overhead on routing.

RFC 1918 address rules in routers and firewalls should seem pretty obvious; however, Section 1.3.2 requires denying those addresses that are specifically designated as internal or private addresses the ability to access the DMZ from the Internet. This should raise a flag in any audit of log files seeing an RFC 1918 address originating from the external port trying to come in to the DMZ or private network. The firewall rule set should only allow valid Internet traffic access to the DMZ. Section 1.3.1 requires restricting traffic from the Internet to only those addresses that are in the DMZ, meaning that Internet traffic may not pass through to the internal, private network. Why can't Internet traffic pass to the internal network? Because Section 1.3.4 requires the database to be on the internal network segregated from the DMZ. The database should never be able to connect directly to the database. Front-end servers or services should only be accessible by the public. These servers and services access the database and return the required information on behalf of the requester just like a proxy. This prevents direct access to the database.

Sections 1.3.5 and 1.3.7 should be tied together in the DSS. Section 1.3.5 requires the restriction of inbound and outbound traffic to that which is necessary for the cardholder data environment. Section 1.3.7 requires denying all "other" traffic whether inbound or outbound that is not specifically allowed. So if you focus on Section 1.3.7 and think about the wording from Section 1.3.5, "that which is necessary," then you should be building a rule set that is only allowing traffic required for business purposes. Everything else would be denied by default.

Again, the DSS doesn't get very granular with the router configurations. Section 1.3.6 requires insuring the router configurations are synchronized. The baseline configuration should be the configuration that is used on a reboot and should also be the current running configuration. No changes should be made to the running configuration without first going through the appropriate change management procedures and changing the baseline configuration first.

Additional firewall considerations should be taken with regards to wireless networks and mobile or personal computers. Section 1.3.8 should be treated just like any other firewall configuration, wired or wireless. Systems with cardholder information must be segregated and all traffic should be denied from wireless networks. In the case of mobile or personal computers, Section 1.3.9 requires a personal firewall for added protection. These units may not always get critical patches in a timely manner and the personal firewall provides some assurance.

Prohibit Public Access

Cardholder data is at the crux of the DSS. We have to protect the data as much as possible. This means not allowing unauthorized access to critical servers that have any information like databases, log files, and trace files. Section 1.4.1 requires a review of the firewall and router configurations to verify that there is not a direct route for Internet traffic regardless if the originating source is internal or public. All traffic must flow through a firewall and router. Section 1.4.2 stresses the implementation of rules on the firewall that restrict traffic from the cardholder applications to only be able to access the servers in the DMZ.

WARNING

There is no reason whatsoever to allow a database or other application to pass traffic past the DMZ to the Internet. This could cause cardholder information to be vulnerable to unauthorized access.

IP Masquerading

IP masquerading is a clever way of saying Network Address Translation (NAT) or Port Address Translation (PAT). It's a security best practice that does not allow your internal address scheme to be seen on the Internet. We use NAT or PAT to accomplish this. NAT is a standard that enables a local area network (LAN) to use a predetermined pool of IP addresses internally and a second set of addresses for external access to the public network creating a many-to-many scheme. The internal pool of IP addresses is, in most cases, derived from RFC 1918. The external addresses are routable, real-world addresses. PAT is a type of network address translation. During PAT, each computer on the LAN is translated to the same IP address, but with a different port number assignment, thus establishing a many-to-one addressing scheme.

NOTE

Either NAT or PAT will work for masquerading. Make sure you test the solution thoroughly before implementing. Some applications may experience adverse effects from one solution or the other.

Choosing an Intrusion Detection or Intrusion Prevention System

Intrusion detection has been around for many years. It's the process of monitoring traffic and activities on systems and networks and then performing an analysis for signs of an intrusion or compromise. Once a determination has been made that an intrusion has occurred, alarms are sent out to the appropriate IT professionals to take steps to correct the problem. In many cases, an IDS is used. But IDSes are passive by design and the results are reactive in nature. Another type of intrusion detection is the Intrusion Prevention System (IPS). IPSes are considered to be the next generation of intrusion detection technology. It not only alerts system administrators of suspect activity, but can also be configured to take corrective actions. IPSs not only prevent known intrusions, but can sometimes prevent unknown attacks based on attack behaviors.

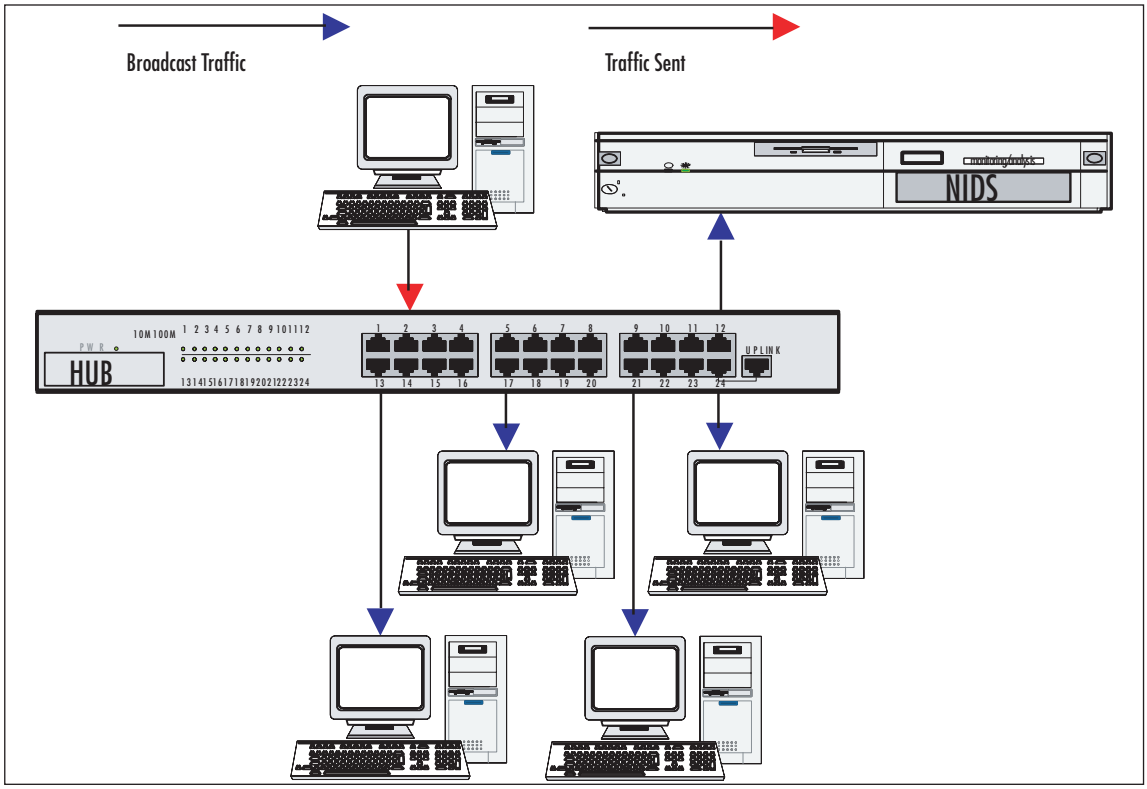
Intrusion Detection Systems

IDSes detect unwanted activity to systems, mainly from the Internet. This activity is usually the product of a hacker executing an attack. IDSes detect malicious activity that can't normally be detected by firewalls, including Trojan horses, worms, viruses, attacks against vulnerable services, unauthorized logins, escalation of privileges, and attacks on applications, to name a few.

IDS can be categorized into several categories:

- **Network Intrusion Detection Systems (NIDS)** An independent platform that examines network traffic patterns to identify intrusions for an entire network. NIDSes need to be placed at a choke point where all traffic traverses. A good location for this is in the DMZ.
- **Host-based Intrusion Detection System (HIDS)** Analyzes system state, system calls, file-system modifications, application logs, and other system activity.
- **Application Protocol-based Intrusion Detection Systems** Monitors and analyzes application specific protocols.
- **Protocol-based Intrusion Detection Systems** Monitors and analyzes the communication protocol between a server and the connected device (another system or end user).
- **Hybrid Intrusion Detection Systems** Combines one or more of the approaches above. In most networks, an IDS is placed in one of three configurations:
- **Hub Configuration** Allows for an easy and affordable implementation. The IDS is connected to a hub in the network segment to be monitored. When traffic traverses a hub, it is broadcasted to all ports, unlike a switch. The IDS can then be connected to any port and monitor the traffic as demonstrated in Figure 4.6.

Figure 4.6 Hub Configuration



- Switch Configurations are very similar to the hub with one major difference. Switch technology is smart in that it only sends traffic to the intended recipient. So in order to allow the IDS to monitor the traffic, a port has to be configured as a mirror or Switch Port Analyzer (SPAN) port. Figure 4.7 shows multiple sessions traversing the switch, inbound and outbound, with the traffic also being sent to the SPAN port.
- Network Test Access Ports (TAPS) allow passive monitoring on a network segment. TAPS are more reliable than hubs or switches and relatively inexpensive to implement. Hubs have a potential for bottlenecks and packet collisions. Switches can also cause bottlenecks depending on the amount of traffic being mirrored to the SPAN port, and have a tendency to not receive error packets. They only receive half of a full-duplex connection and handling Virtual Local Area Network (VLAN) can be complex or impossible. The TAP configuration shown in Figure 4.8 alleviates these problems and is

completely passive, doesn't cause bottlenecks or packet loss, and supports full-duplex.

Figure 4.7 Switch Configuration

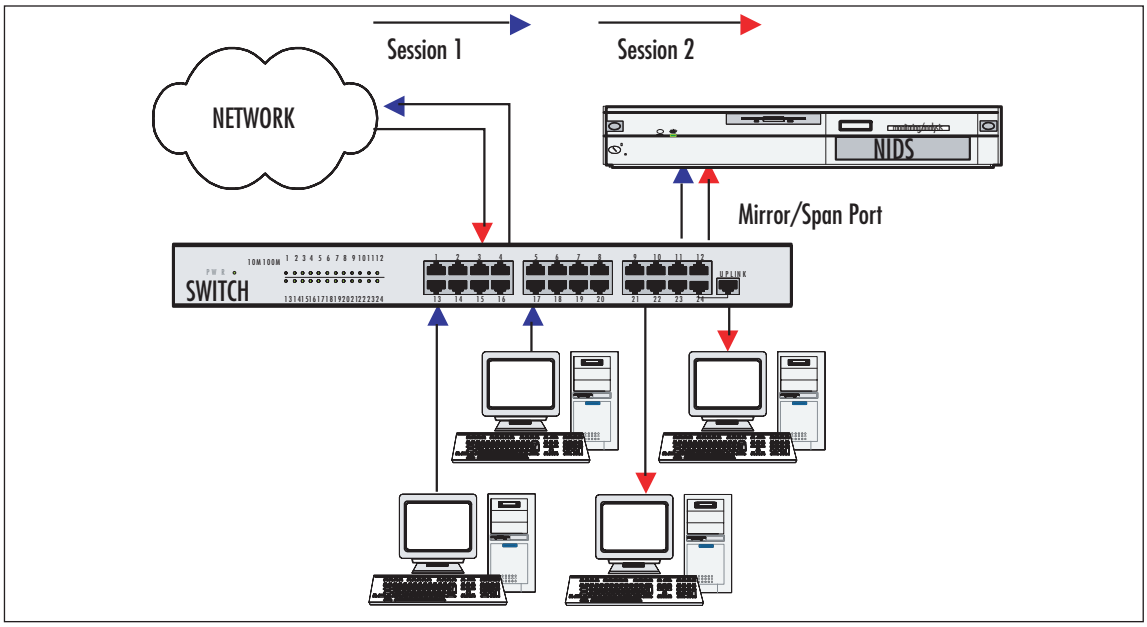
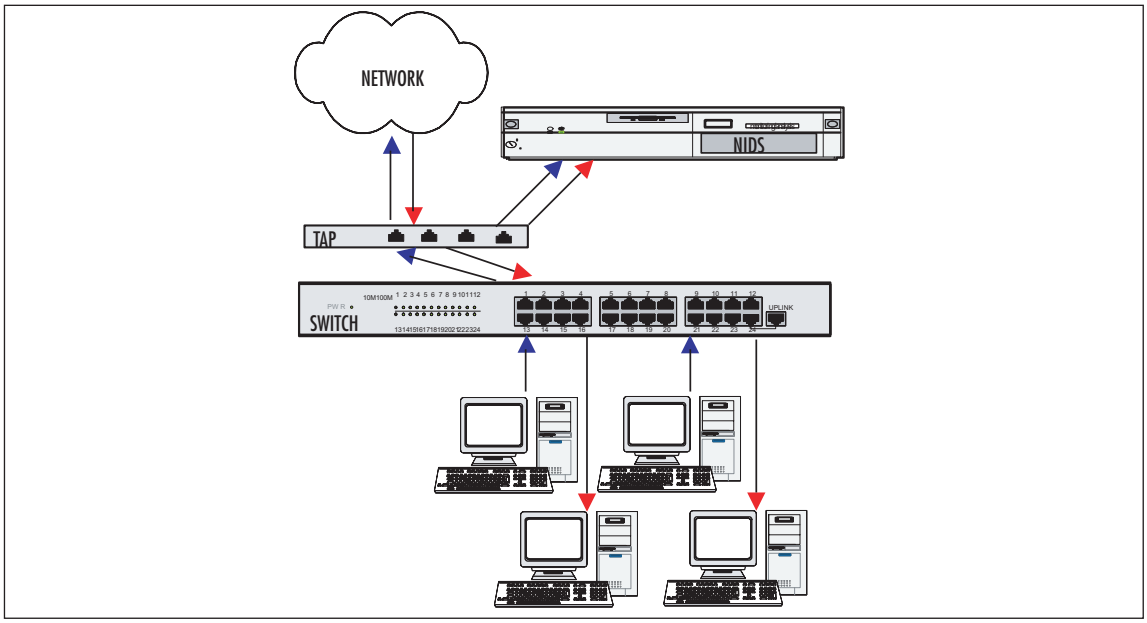


Figure 4.8 Network TAPs



Intrusion Prevention Systems

The IPS is considered, by most security professionals, to be the next generation of IDS. It provides configurable thresholds and policies for network traffic and an IDS for sending suspect activity alarms to network administrators. An IPS makes attempts to stop and attack, whereas an IDS only alerts you to the potential attack. Currently, there are two types of IPSs:

- Host-based Intrusion Prevention systems (HIPS)
- Network-based Intrusion Prevention systems (NIPS).

HIPSes protect workstations and servers through software that resides on the system. HIPSes catch suspect activity on the system and then either allow or disallow the event to happen, depending on the rules. HIPS monitors data requests, read or write attempts, and network connection attempts to name a few.

NIPS is a network security solution. NIPSes monitor all network traffic for suspect activity and either allows or disallows the traffic to pass. For a NIPS to work properly, it needs to be positioned in-line on the network segment so that all traffic traverses through the NIPS. The implementation of a NIPS is similar to a NIDS with one exception. Since a NIPS has two NICS, a network TAP, switch, or hub is not required. The network only needs to be architected with the NIPS in a position where it can monitor all the network traffic inbound and outbound.

NOTE

IDSes are reactive in nature. They only monitor and send alerts of suspect activity. IPSes not only alert, but can take action to mitigate the problem.

Again, the DSS does not dictate which solution should be used. In many cases, this may come down to cost. Both the IDS and IPS have their advantages and disadvantages and should be weighed accordingly. If I had my way, I would go with a combination of a NIPS solution placed in a DMZ to eliminate the need for a TAP, hub, or switch. It also has the added feature of being able to take corrective actions once configured and then utilize a HIPS on critical systems.

Antivirus Solutions

Antivirus software is a basic necessity for all systems and networks that have an Internet presence. It's even more important to the PCI because of the customer information that is being stored. Antivirus software also adds another layer to your overall security. The distinct characteristics that, at one time, made viruses, worms, Trojans, and spyware unique from one another is not so clear anymore. I'll use the term malware to encompass them all. Although many malware programs are more of a nuisance than cause any real damage the threat still exists and the risk of having your customer's credit card information stolen is high.

Gateway Protection

E-mail is one of the primary vehicles that malware uses to spread throughout the Internet. Adding an antivirus solution that runs on your e-mail server or Simple Mail Transfer Protocol (SMTP) gateway that scans each message before passing the message to the intended recipient helps to protect your users and your data and systems. Gateway antivirus solutions provide a balance with the need to communicate over the Internet quickly and the need to protect the privacy and integrity of information and services. Gateway solutions reduce the threat of viruses entering a PCI network, and also reduce the likelihood of internal individuals being able to send viruses to Internet users.

Desktop and Server Protection

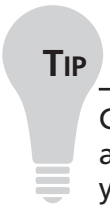
The desktop cannot be ignored. This is where most of the problems exist. Users receive e-mails and bring disks to work that may be infected. By having antivirus software installed on every desktop, in addition to the gateway protection, protects the user from receiving infected e-mail or inadvertent downloads of malware.

There was a time when system administrators didn't want to put antivirus software on their servers because of performance issues. That rationalization will get you in trouble quickly. Just because you have gateway antivirus solutions and all of the users have antivirus software on the desktop doesn't make the servers immune. Malware can spread throughout an enterprise, and in most cases, doesn't care if it touches a server or PC.

For an antivirus solution to be effective it must be:

- Installed and running on every laptop, desktop, and server at system boot. The software should be password-protected so that users cannot disable or uninstall the application. It may sound trivial, but users and administrators disable antivirus software all the time because it slows down their system. Therefore, password-protecting the administrative functions of the software has become a necessary evil.
- The solution should also provide real-time scanning. Most of us are familiar with static scanning. That is when your desktop automatically starts a weekly scan of your hard drive or when you execute a manual scan of files on your system. Real-time scanning scans all files that the operating system uses before it is fully opened.
- The antivirus solution must be kept up-to-date with the latest signatures. New malware is being released daily. If your antivirus solution is not current, the users and data are at risk. Auditors will check the signature time stamps to make sure they have been updated.

Most enterprise level antivirus solutions provide protection for servers, desktops, and the gateways with an administrative console to download the latest signature files and push them to the systems. A couple of the better known manufacturers are Symantec and McAfee. Make sure you do your due diligence and research all of the solutions available and make the right choice for your organization.



TIP

Consider using multiple vendors for your antivirus solution. An enterprise antivirus suite may not provide the layered security you require to protect your systems and data. Having one vendor solution for the gateway and another for the servers and desktops is acceptable. They are only as good as their latest signature files and their ability to detect "malware-like" activity.

System Defaults and Other Security Parameters

A lot of thought goes into securing a network. Not only do you have to think about the network devices (e.g., routers, firewalls, IDSes) and antivirus software, you have to

think about system defaults, configuration management, and encrypting non-console administrative access to name a few. Many of these do not contain a lengthy explanation; however, from a best practices standpoint it should be done to increase your security posture.

Default Passwords

Default passwords exist with almost every operating system and application. Section 2.1 of the DSS requires that all vendor-supplied passwords be changed before deploying a system on the network. Section 2.1.1 requires the same for wireless environments. System passwords are usually a set-and-forget thing, but it is good practice to change them at least quarterly. Password policies and procedures are usually dictated by the organization. Although there are several alternatives for authentication like biometrics, Smart Cards, and tokens, most of us use the traditional ID and password.

Additionally, if your organization has a procedure for adding new users to the network and granting them access to systems, there may be some default passwords that you haven't thought about. If you can remember back to when you first received your user ID and password, you might recall that it was a preset generic password. There is a very good chance the system administrator's use that same password for all new users. Therefore, those accounts need to be taken into consideration from a security perspective and appropriate actions taken.

A strong password policy and enforcement will help to protect the systems form potential compromise. Here are some simple password rules, above and beyond changing default passwords that will provide stronger security.

- User-level passwords must be changed at least every 60 to 90 days.
- Accounts that have system-level privileges must have a unique password from all other accounts held by that user.
- Passwords must not be transmitted over the Internet by e-mail or any other form of communication, without being encrypted.
- Passwords should be a minimum 6 to 8 characters in length, with a combination of upper- and lower-case alpha and numeric characters and special characters as well (e.g., !%@$)
- Passwords should never be written down or shared with anyone.

SNMP Defaults

Sections 2.1 and 2.1.1 require all system defaults to be changed before deploying a system onto the network. The Simple Network Management Protocol (SNMP) strings must be changed. SNMP is associated with several known vulnerabilities. SNMP is a good network management tool for administrators. It gives them the ability to touch a device across the network. That being said, it allows hackers to do the same. Make sure SNMP defaults are changed.

The most basic form of SNMP security is the community string. There is a public community string that provides read-only access to network devices. The default value for this community string is usually "public." Remember, community strings are not unlike passwords. Using this community string like a password, the Network Management System (NMS) can retrieve data from network elements.

WARNING

The only thing worse than having "public" as your community string, is to have no community string at all. This would give anyone at least read access to your network devices. A hacker can find out a lot of information about a device through SNMP.

Delete Unnecessary Accounts

Out of the box, systems and applications come with a variety of accounts preinstalled. Some are system accounts and others are administrative accounts for support from the vendor. It is my recommendation that any support account be deleted immediately. These are like backdoors into your system—if not controlled closely, they can be disastrous. All guest accounts should be deleted or at least disabled. The passwords should be set to something no one knows and you should consider renaming the account if it can't be deleted. The same goes for default administrator accounts. Rename them to something inconspicuous. Name them something that conforms to your organization's naming standards and change the description of the account as well. It adds a layer of difficulty for an attacker looking for the account.

Wireless Considerations

Wireless networks should be treated the same as a wired network when it comes to security with a few hooks. Wireless stretches the boundaries of your network past the brick and mortar walls and out where you don't have control over who attempts to connect to your network. You can prevent someone from gaining unauthorized access by changing the default settings.

Remember to change the default passwords. Some of the more obvious defaults to change are:

- Change the Wireless Equivalent Privacy (WEP) key at least monthly. WEP keys are inherently weak.
- Change the default Service Set Identifier (SSID). The SSID is the network identification. SSIDs are easy to crack and most vendors use the same or similar SSID for all of their models. When changing the SSID, choose one with little or no meaning. Don't name it the organization name and don't broadcast it, thereby making it less obvious and less accessible.
- Enable WiFi Protected Access (WPA and WPA2) for encryption. For the WPA pre-shared key, create a key that's not easily compromised. Keys can usually be entered as a pass phrase, hexadecimal characters, or manual hexadecimal values.

NOTE

WPA provides a greater security than WEP. If possible, do not consider WEP as a viable solution.

Notes from the Underground…

WEP has been proven to be a very weak encryption technique to secure a wireless connection. The article, "Breaking 104 bit WEP in Less Than 60 Seconds," (http://eprint.iacr.org/2007/120.pdf) discusses how easy it is to break WEP. In a nutshell, there is a 3-byte vector called an Initialization Vector (IV). The IV is prepended onto packets based on a pre-shared key that all clients that need to authenticate must know. For most WEP hacks, you will probably only need tools like kismet, airodump and aircrack. These tools are available for download on the Internet. Once you find the network, you need to start capturing IVs. Airodump is my tool of choice for packet capturing. After the packets are gathered simply run aircrack against the appropriate file; you should have a crack in a relatively short period of time. Notice I didn't get into the configuration of the tools. Most are default configurations and help is available on the Internet.

Develop Configuration Standards

All organizations should adopt a practice that is considered to be a minimally acceptable configuration practice for all systems. It is a key element of a security and aids a security team's efforts in reducing the vulnerabilities on their systems and the overall risk to the organization. Section 2.2 requires that all known security weaknesses are addressed and are consistent with industry-accepted system hardening standards defined by the National Institute of Standards and Technology (NIST) and the Center for Internet Security (CIS), to name a few. If a particular vulnerability is not addressed with specific hardening techniques, workaround solutions may need to be applied to mitigate the risk. Once you have adopted a standard, the systems should be baselined to ensure all systems are built and hardened the same every time.

Creating security baselines on computers and your networks is no trivial task. It takes time and effort, but the end result is priceless. A security baseline is a standard set of security settings that are established for each type of computer or network component in your organization. The baseline configuration is a "point-in-time" configuration and should be updated regularly as new settings are applied. Your orga-

nization's security policy should drive what security is applied to your systems. A well-defined security policy will lay the foundation of what security must be put in place.

Implement Single Purpose Servers

Subsection 2.2.1 requires that critical servers provide a single service (e.g., DNS, database, e-mail, Web) to the organization. All too often, organizations try to save money by hosting multiple server services on the same host. Each service brings its own vulnerabilities and risks to the table and provides a hacker with multiple choices for attack. If too many services are provided by a single server, an exploited vulnerability on one service (i.e., DNS) can bring down or cause a denial of service (DoS) to the entire server. The integrity of all the services and data is questionable at that point. As a rule of thumb, the more services provided on a single host degrades the overall security of the server and the organization.

NOTE

If you are running a Web server that is interacting with a database, that Web server should always reside on its own host.

Configure System Security Parameters

You might think this is a "no brainer," but not all system administrators know exactly what is enabled and disabled on their systems and how the system itself is secured. Section 2.2.3 requires the verification of all system security parameters to prevent misuse. This particular control is a question and answer session with the system and security administrators. Section 2.2.3 lists the following procedures:

1. Interview system and security administrators to verify that they have knowledge of common security parameter setting for their operating systems, database servers, Web servers, and wireless systems.

TIP

Don't forget about your network appliances and peripherals. These should also have appropriate security features applied.

2. Verify that common security parameter settings are included in the system configuration standards.

This goes back to Section 2.2, developing configuration standards for all systems and components. A baseline security configuration needs to be established. Baseline security standards substantiate the security of your organization and the information you must protect. Implementing the security features required by your security policy, or implementing the security policy is often easier said than done. Fortunately, NIST provides checklists for almost all platforms in use today that are freely available on their Web site, http://checklists.nist.gov/repository/index.html. If you follow a standard and create a baseline configuration, then all servers, computers, and components on your network should have the same settings as applicable.

Disable and Remove Unnecessary Services, Protocols and Functionality

All unnecessary and insecure services and protocols should be disabled as required by Section 2.2.2. Simply stated, what this means is if there is not a valid business case for having a service or protocol active, it should be disabled. This also applies to Section 2.2.4. All unnecessary functionality, such as scripts, drivers, subsystems, Web servers, and so forth, should also be removed. More and more industries are practicing this. If it's not needed, get rid of it. It will save you the headache down the road of having to explain why it was there in the first place if the organization doesn't use it.

NOTE

Remember, in most cases default installations have numerous vulnerabilities. A lot of these services, features, ports, protocols, and so forth were put there by the vendor and it is well-known information that is freely available on the Internet.

Encrypt Non-console Administrative Access

System and network administrators, by design, have access to everything. They "own" the network. However, some of the tools they use are a little less than secure. Many of the tools are antiquated and actually pass user IDs and passwords in the clear. To accommodate the requirement of Section 2.3, encryption solutions must be used for

all non-console administrative access. Think about this. If you are going to require your administrators to utilize encryption for services such as Telnet, it would be a good idea to make all the users in the organization use an encrypted solution for Telnet such as SSH.

To meet this requirement, three things have to happen.

- SSH (or other encryption method) has to be invoked before an administrator's password is requested.
- A review of services and parameter files on systems to determine if Telnet or other remote log-in commands are not available for use internally (e.g., the "r" commands in Unix. (i.e., rlogin, rsh, ruptime, rcp, rwho).
- The administrator access to any wireless management interfaces must be encrypted with Secure Sockets Layer/Transport Layer Security (SSL/TLS). Additionally, it must be verified that administrators are not allowed to connect to the wireless management interface remotely. They can only connect from a management console.

Hosting Providers Must Protect Hosted Environment

PCI compliance goes further than just the commercial entity providing the goods and services. Far too often your favorite store is nothing more than a "store front" with no back office, just a building or a Web site that pushes goods. All of the databases and Web site hosting is done through a service provider. Section 2.4 requires that hosting providers protect each entity's hosted environment and data.

Summary

All systems must be protected from unauthorized access, whether it is from the Internet or any other source. What seems like an insignificant path from the Internet, employee e-mail, and browsers or e-commerce services such as Web servers can prove to be disastrous if not secured appropriately. Throughout this chapter, we have discussed two requirements of the PCI DSS: Requirement 1, Install and maintain a firewall configuration to protect cardholder data, and Requirement 2, Do not use vendor-supplied defaults for system passwords and other security parameters. Understanding these two requirements is fairly easy. Complying with them or actually implementing the required security features can be somewhat overwhelming.

The standard for the type of firewall that is acceptable to meet the PCI standard was stated for you. It must provide dynamic packet filtering (only "established" connections are allowed through the firewall) commonly known as stateful inspection. The firewall configuration must be managed at all times. Router configurations must be managed as well. Section 1.1.8 states that the configuration standards for firewalls and routers must include a quarterly review of their rule sets. Any unneeded ports, protocols, and services must be removed or disabled. All management functionality, including groups, roles, and responsibilities, must be through a secure means and be thoroughly documented in the organization's security configuration standards. If there isn't a valid business case for having it, get rid of it.

We also discussed administrative access to systems and components. Remote access to critical servers should not be allowed. If access to a device, whether it's wired or wireless, is required, it must be through an encrypted connection. Otherwise, administrators should only use an appropriate management console to perform the required tasks.

The trend for these two requirements was to have configuration standards implemented. Configuration standards must take into consideration all network devices (i.e., firewall, routers, switches, IDSes) and your computers, servers, services, and applications. Default configurations and passwords are almost always published on the Internet. For this reason alone, we need to take precautions and change all default setting so as not to make the attacker's job easy. If an attacker makes attempts to exploit your environment and finds it difficult, chances are he'll move on to something easier.

Configuration standards mean baselining. Once the different types of systems and components have been hardened, a baseline security configuration should be estab-

lished. This takes the guess work out of building and configuring the next, like, system. It will have the same configuration as the previous one if the baseline configuration is followed. The baseline security configuration should be updated on a periodic basis to include new changes to the system, and should always follow what is stated in the configuration standards and required by your organization's security policy.

Solutions Fast Track

Installing and Maintaining a Firewall Configuration

- ☑ The PCI DSS requires a firewall that provides stateful inspection, also known as dynamic packet filtering.
- ☑ Stateful inspection firewalls offer strong security along with good performance and transparency to end users, unlike the packet filtering and proxy firewalls.
- ☑ Document your dataflow in order to aid the system and security administrators in configuring the firewall with the proper rule set.
- ☑ Disable or remove all unneeded ports, protocols, and services not required for business purposes.
- ☑ Deny all traffic into and out of the firewall that is not required for business purposes.
- ☑ Your firewalls and routers must have documented configuration standards and the rule sets of each should be reviewed at least quarterly.

Choosing an Intrusion Detection or Intrusion Prevention System

- ☑ IDSes differ from IPSes in that they will only send alerts to the administrators if suspect activity is detected. An IPS will take corrective actions.

- ☑ A network TAP provides the best possible connection point for any type of intrusion detection solution. It eliminates potential bottlenecks and dropped packets.
- ☑ IPS solutions are considered the "next generation" of intrusion detection and, when properly configured, will take corrective actions in addition to alerting appropriate personnel.

Antivirus Solutions

- ☑ A good antivirus solution protects against virus attacks at the gateway and also at the server and desktop.
- ☑ Gateway antivirus solutions provide a balance with the need to communicate over the Internet quickly, and the need to protect the privacy and integrity of information and services.
- ☑ For an antivirus solution to be effective, it must be installed and running on every laptop, desktop, and server at system boot. It must also provide real-time scanning and be kept up-to-date with the latest signature files.

System Defaults and Other Security Parameters

- ☑ All default passwords must be changed before deploying a system on the network.
- ☑ The public string in SNMP, if used, must be changed to something unique. It should never be left as "public" or blank.
- ☑ All accounts provided in a default installation should be deleted if not required for business purposes.
- ☑ WPA should be enabled for encryption on wireless access points rather than WEP. WEP keys are inherently weak.
- ☑ Develop security configuration standards for all of your systems and baseline your configurations.

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to **www.syngress.com/solutions** and click on the **"Ask the Author"** form.

Q: What type of firewall is best suited for complying with PCI standards?

A: The PCI DSS states in Section 1.3.3, that the firewall solution must provide stateful inspection.

Q: What type of architecture should one choose for PCI compliance?

A: The PCI standard does not dictate this, but the industry best practices are to have screened subnets (DMZs) or possibly a dual firewall configuration.

Q: What services, ports, and protocols are allowed to be active in a PCI environment?

A: The only services, ports, and protocols that are allowed are those that are required for business purposes. These must be secured and documented appropriately. If a protocol other than HTTP, SSL, SSH, and VPN is required, justification must be provided.

Q: Is one intrusion detection solution preferred over another?

A: Both IDSes and IPSes have their advantages and disadvantages. An IPS, however, has the capability of not only sending an alert like an IDS, but also taking corrective action if configured appropriately.

Q: Is there a requirement for a specific type of intrusion detection solution?

A: No, the PCI standard only requires that either an IDS or IPS be in place and provide monitoring and alerting of suspect activity.

Q: If the functionality of an IPS to take corrective actions is not required, why spend the money to implement an IPS?

A: An IPS solution provides the ability for corrective actions to be taken before a system administrator has the opportunity to respond.

Q: Are there any antivirus solutions that are considered better than another?

A: All antivirus solutions provide certain levels of security to the enterprise. When choosing a solution, make sure it is manageable from a central console, can be password-protected on each host, and has the ability to provide gateway protection. It is not uncommon for different vendors to be used for the gateway protection and the rest of the enterprise.

Q: At a minimum, what accounts need to be removed from my systems before deploying them onto the network?

A: All accounts that do not have a valid business case must be removed. Default accounts are often the targets of attack by hackers.

Q: My wireless access point only provides WEP. Is this acceptable?

A: Per the PCI standard it is acceptable, but the key should be changed at least monthly. Consider upgrading to a device that provides WPA for added security.

Q: My organization doesn't have a particular security configuration standard. Is there anywhere I can go to find information on this?

A: NIST, CIS, and SANS all provide standards and guidance on security configuration standards. NIST provides checklists that are freely available on their Web site, http://checklists.nist.gov/repository/index.html.

Q: Can I run services like Telnet or rsh on my internal network as long as it's not accessible from the Internet?

A: You should only have these services available if there is a valid business case. The PCI standard clearly states that all unneeded services be removed. These legacy services are not secure by any means. If required, a more secure solution should be used like SSH.

Chapter 5

Protect Cardholder Data

Solutions in this chapter:

- **Protecting Data at Rest**
- **Protecting Data in Transit**
- **Compensating Controls**
- **Starting with a Strategy**
- **The Absolute Essentials**

- ☑ **Summary**
- ☑ **Solutions Fast Track**
- ☑ **Frequently Asked Questions**

Protecting Cardholder Data

The Payment Card Industry (PCI) Data Security Standard (DSS) requirement to protect cardholder data encompasses two elements:

- Protect stored cardholder data
- Encrypt transmission of cardholder data across open, public networks

The processes and activities necessary to meet these requirements and the specific sub-items spelled out by the PCI DSS, are simply the implementation of some of the fundamental components of a sound information security program. If you have already put into place the pieces of a solid information assurance program, or you are in the process of doing so, there won't be a great deal of extra work to do. Your current processes and technology may very well serve to quickly allow you to comply with these requirements without a great deal of additional effort or cost.

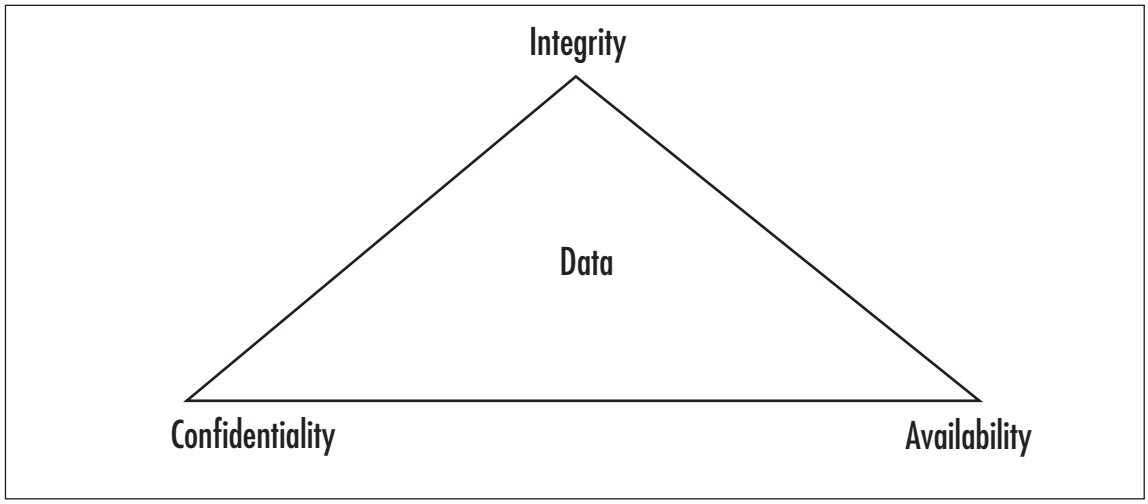
In the arena of Information Security (Infosec) there are three fundamental tenets that form the basis for evaluating the effectiveness of the security controls we employ to protect our data. These three tenets are Confidentiality, Integrity, and Availability (CIA). Let's discuss these briefly, as we will refer to them as we delve into the specifics of protecting cardholder data.

The CIA Triad

These three tenets of information security are referred to as a triad, because they are most commonly illustrated as three points of a triangle. (See Figure 1.1) All three principles must be considered as you manage your data. An undue degree of emphasis on one can lead to a deficiency in one of the others.

- **Confidentiality** Strives to ensure that information is disclosed to only those who are authorized to view it.
- **Integrity** Strives to ensure that information is not modified in ways that it should not be. This can refer to modification by either people or processes.
- **Availability** Strives to ensure that data is available to the authorized parties in a reliable and timely fashion.

Figure 5.1 The CIA Triad



PCI Requirement 3: Protect Stored Cardholder Data

The most effective means of insuring that stored cardholder data is not exposed to unauthorized parties (confidentiality) is the encryption of that data. When implemented properly, the value of encryption is that even if an intruder is able to gain access to your network and your data, without access to the proper encryption keys, that data is still unreadable.

PCI standards dictate that stored cardholder data be rendered unreadable (encrypted), but allow you to implement compensating controls to mitigate the risk if you are unable to meet this requirement. Since encryption is such an effective and critical part of protecting data, we will discuss some of the details of encryption methods and the associated advantages and disadvantages.

Encryption Methods for Data at Rest

Disk encryption software can be broken down into two high level categories:

- File- or folder-level encryption
- Full disk encryption

Another option for encryption of key cardholder data is database (column-level) encryption.

Let's examine the advantages and disadvantages of each as you consider how and where they might fit into your program for protecting cardholder data.

File- or Folder-level Encryption

File- or folder-level encryption (or file system level) is an encryption system where specific folders, files, or volumes are encrypted by a third-party software package or a feature of the file system itself.

Advantages

- More granular control over what specific information needs to be encrypted can be accomplished. Items that you desire to be encrypted can be stored in a particular folder or volume, and data that does not need to be protected can be stored elsewhere.
- Many file-level encryption products allow you to integrate access level restrictions. This allows you to manage who has access to what.
- When data is encrypted on a file level and is moved off the storage location, it is moved encrypted. This maintains the confidentiality of the data when it is moved to a backup tape.
- Less invasive to a database than column-level encryption. The schema of the database does not need to be modified and the access of data by authorized personnel (based on access control) is not hindered when querying and other management activities take place. This is an aspect of *availability*, one of the three tenets of the CIA triad.
- Tends to consume less resource overhead, thus less impact on system performance.
- Logging and auditing capabilities. Some file-level encryption systems offer the capability to track who attempts to access a file and when. Since the majority of data breaches are internal to the network, this kind of information is good to have.

Disadvantages

- Can cause performance issues for backup processes, especially with relational databases.
- Requires extra resources for key management.
- May not be granular enough when access to certain columns of a database is desired, but others need to be restricted.
- Possibility of encrypting more data than is necessary for PCI compliance.

Full Disk Encryption

Full disk encryption (FDE) or "whole disk" encryption methods encrypt every file stored on the drive (or drives), including the operating system/file system. This is usually done on a sector-by-sector basis. A filter driver that is loaded into memory at boot, encrypts every file as it is written to disk, and decrypts any file that is moved off of the disk. This happens transparently to the end user or the application generating the files.

Advantages

- Everything on the drive (or drives) is encrypted, including temporary files and swap space, increasing security of your data.
- Encryption of data is enforced on end user, alleviating decisions on what or what not to encrypt.
- Encryption/decryption is transparent. When information needs to be accessed, it can be saved off of the system and is automatically decrypted.
- Most FDE systems offer support for pre-boot authentication, which can add another layer of protection to the method.
- Since all data on the drive is encrypted, even if an alternative boot media is used against an encrypted system, the data on the drive is unreadable and therefore useless to the thief.
- Hard tokens, soft tokens, or passwords can be used in most cases for the pre-boot authentication process that allows access to the system.

Disadvantages

- Some FDE programs can cause an increase in data access times. Slight delays in writing and reading data can occur, especially with very large files.
- When FDE systems encrypt on a sector-by-sector basis, fragmentation on the drive can cause significant problems.
- Encryption key management has to be considered. If a key for recovery of data is stored offline, end user support processes for recovery of data need to be put in place.
- Password management processes have to be defined and put into place. If a user loses their password that grants access to the encrypted system, they have no access to their data. This would impact the availability of the data as referenced in the CIA triad model.
- With FDE systems, once a user is authenticated to the system via the password used for the encryption software, full access to all data is achieved. This puts increased emphasis on insuring that strong password or pass phrases are utilized for the pre-boot authentication.
- If the encryption software becomes corrupted or otherwise fails and can't be recovered with the unique recovery key, the data on the drives cannot be recovered. The only option is to reformat the drive. While this protects the data, it tends not to be very popular with end users.

Implications

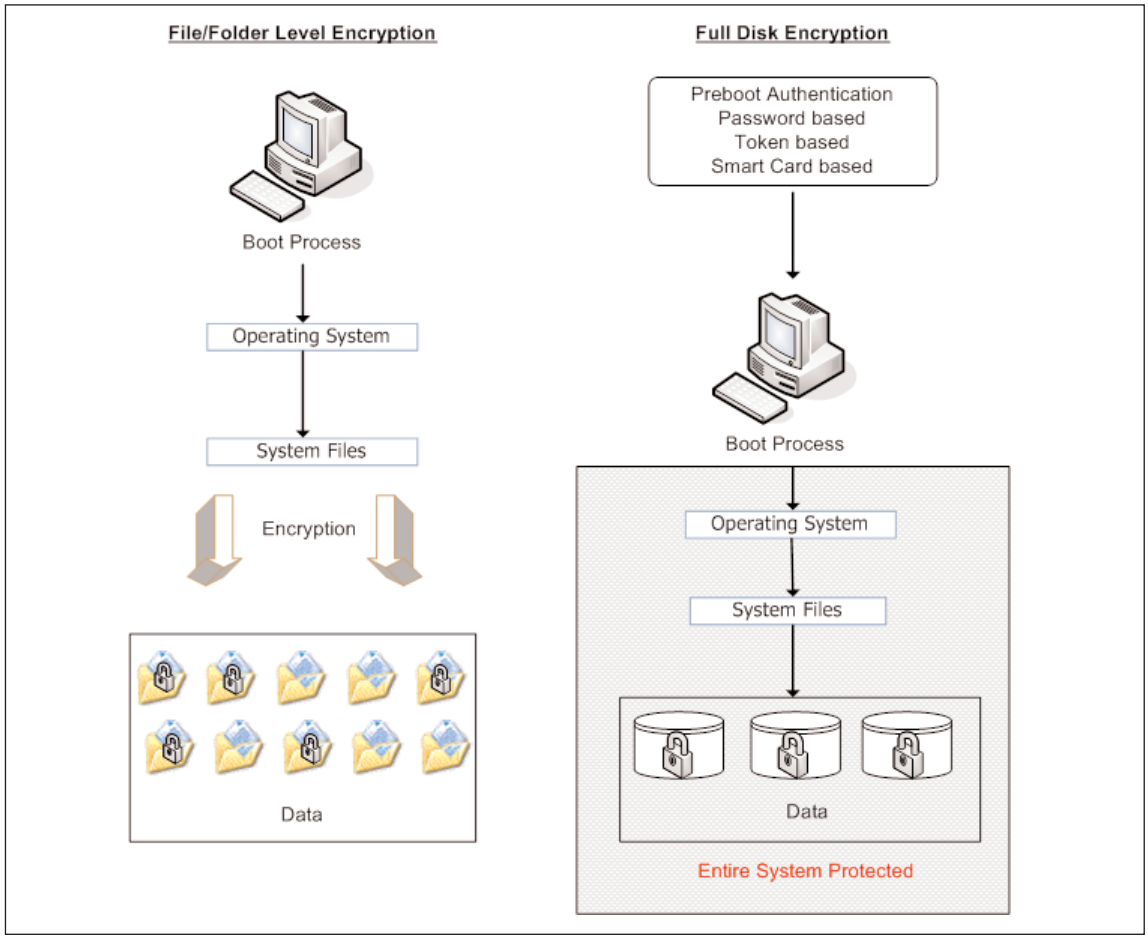
In order to ensure that stored cardholder data is protected from access by unauthorized parties, it is likely you will need to utilize both file-level encryption and FDE in your enterprise environment. In addition, access controls around databases and possible column-level database encryption may be needed. Every environment is different. What you need to do will be dependent upon your network and your current design.

FDE is more suited to protecting data on workstations and mobile devices, whereas file-level encryption is more useful as a method on storage devices. A well-designed information assurance program will prohibit storage or transfer of sensitive data to an employee's laptop or desktop. While this kind of policy and practice would seem intuitive and obvious, it is abundantly clear that such practices are not always

followed strictly. The much publicized cases of database managers or analysts putting thousands of clients at risk, because a laptop was stolen which had been used to download large volumes of sensitive data from a storage device, only serves to demonstrate this fact.

Figure 5.2 illustrates the difference in architecture between file-level encryption and FDE.

Figure 5.2 File Based Encryption vs. Full Disk Encryption



Database (Column-level) Encryption

Ultimately, the most crucial element of cardholder data that needs to be rendered "unreadable" wherever it is stored, is what PCI DSS refers to as the Personal Account Number (PAN). This is the full account number that identifies both the issuer of the

card and the cardholder account. PCI DSS 3.4 states "The MINIMUM account information that must be rendered unreadable is the PAN."

This is not to say that other elements of cardholder data would not benefit from being encrypted. But since this data is necessary to be stored, it needs to be protected. Other items of data pulled from a card during normal business are never to be stored, and thus should not be residing in a stored database.

Column-level encryption allows a more granular approach to rendering the key cardholder data unreadable, by focusing on the specific data that needs to be protected.

Advantages

- When a table is queried for data in a non-encrypted column, no performance impact is seen. Since no decryption activity is taking place, no delay in reading/writing and no performance hit by system due to encryption software activity is seen
- When a query for a record with data from an encrypted field is performed, the overhead is minimal. Since the decryption activity only has to take place on the individual field or fields that are encrypted, there is much lower overhead.
- It can be used in conjunction with other controls to protect data from administrators. Separation of duties between security administrators and database administrators reduces the risk presented, by allowing a database administrator (DBA) unlimited access to the data you need to secure for PCI compliance.

Disadvantages

- Requires tight integration with the database.
- It is highly invasive to the database design. To implement column-level encryption protection after the fact you will likely have to change the following:
  - Data type of the field being encrypted.

  - References to, and queries of the encrypted field(s) will have to be modified to limit access. Middleware and other applications that interact with the database will have to be comprehended and possibly reconfigured.
- Key management has to be well planned. If the encryption key is hard-coded into scripts, it defeats the security. Keys themselves must be stored in an encrypted state and access controls placed around them.
- Employing column-level encryption can lead to a false sense of security. Merchants and service providers who perform batch processing will commonly end up storing sensitive data in flat files. Additionally, sensitive data is often found in debug and transaction logs. The column-level encryption does not protect this; only file-level encryption would. It has to be remembered that the column that the sensitive data is entered into may not be the only place it is stored. PCI DSS requires it to be rendered unreadable wherever it is stored.

Overview

The pursuit of protecting data from being exposed to unauthorized parties is rarely accomplished on a single level. As will all strong information assurance programs, the best approach is to think "defense-in-depth." Multiple layers of protection are what guard you from having your plan and procedures defeated through a single point of failure. Column-level encryption might be the answer for a piece of your overall plan for compliance to protecting cardholder data, but it is unlikely to be the entire plan.

Other Encryption Method Considerations

File-based encryption, FDE, and column-level encryption are the most well understood and the most commonly employed types of data encryption at this time. There are other possible solutions you need to be aware of, although the cost and design implementations may be more prohibitive.

Storage-level Encryption

Storage-level encryption is a hardware-based solution and is beneficial for encryption on the file level and directory level, and lends itself well to encryption of removable media and tape media. If your concern is that you are storing sensitive data and you don't want or need to have the granularity of what is or is not encrypted, this could be of benefit.

Encryption Appliances

If you choose to implement a hardware-based solution for simply protecting tape storage or to encrypt data as it flows between multiple devices, the one advantage that it brings is the reduction of resources for key management. Keys never leave the encryption appliance. Scalability is also a factor, as additional appliances can be added to the locations desired ad design and growth change.

WARNING

Don't' forget about portable storage devices that attach to laptops or desktops. Full disk encryption implemented with accompanying pre-boot authentication is the best way to protect data on a mobile system such as a laptop. What can undermine the protection, however, is the use of Universal Serial Bus (USB) storage devices, which can be easily attached and removed with sensitive data. There are some software-based solutions that can be configured to enforce encryption on any attached USB device. This can create hardship in some aspects, but it can also protect you from having your expensive encryption solution undone by a careless employee who stores sensitive data on an encrypted system, but then uses a non-protected USB drive to transfer the data, thus decrypting it as it is transferred to the device.

PCI Requirement 4—Encrypt Transmission of Cardholder Data Across Open, Public Networks

As in the case of protecting stored data, the most reliable and efficient way to ensure that your transmitted data is not intercepted (confidentiality) or modified (integrity), is to encrypt it during transmission. PCI Requirement 4 spells out some specific details as it relates to these procedures for communication.

Let's take a look at some of the specific PCI DSS sub-items in order to illuminate some of the terminology and the implications.

Requirement 4.1—Cryptography and Protocols

This requirement states "Use strong cryptography and security protocols such as secure socket layer (SSL)/transport layer security (TLS) and Internet protocol secu-

rity (IPSec) to safeguard sensitive cardholder data during transmission over open, public networks."

An open, public network is essentially any network that contains any kind of gateway device that provides clients on that network wired connectivity to the Internet at large. This describes the networks of pretty much every business today. Anytime your cardholder data is transmitted over the Internet or any network you are unsure is secure, that data has to be protected.

The PCI DSS documentation specifically refers to the following as examples of open, public networks:

- The Internet
- Wireless Fidelity (WiFi)
- Global System for Mobile Communications (GSM)
- General Packet Radio Service (GPRS)

Let's take a look at the specific protocols involved with securing data when transmitted over these various types of networks, and the way they are applied.

SSL/TLS

SSL refers to a protocol for message transmission known as secure sockets layer, and TLS refers to the protocol that recently superseded it known as transport layer security.

SSL on Web Servers

If you are hosting sensitive data on your Web site, you can protect the data by acquiring a digital Web server certificate and installing it on the Web server. Then you must be sure to allow traffic through your firewall on port 443, as this is the default port that SSL communications use.

SSL on E-mail Servers

SSL protocol can also be used to secure e-mail. This also entails the process of installing a digital certificate on your e-mail server. It's important to remember that this only causes your Simple Mail Traffic Protocol (SMTP) traffic to be encrypted in transit. The actual e-mail message and attachment will not be. This is where file-based encryption would be of value.

About TLS

Describing the technical differences between TLS and SSL is beyond the scope of this chapter. However, it works in much the same fashion as SSL does, and it is important to be aware of the following:

- TLS is the successor of SSL.
- TLS is best for direct SMTP communication between two e-mail gateways. The contents of the e-mails as well as the communication stream between them are encrypted.
- Most modern Post Office Protocol (POP) and Internet Message Access Protocol (IMAP) e-mail client programs also support TLS. If the client is utilizing TLS, the contents of their messages are also encrypted when sending e-mail to your TLS-enabled e-mail server.

WARNING

Be aware that TLS only protects your e-mail messages between two TLS-enabled e-mail servers. If there are intermediate hops between the two gateways where your e-mail is relayed, the encryption is lost after it is forwarded to the next gateway.

Securing Wireless Networks Transmitting Cardholder Data

Wireless networks are becoming much more common in the business (and home) community. Unfortunately, the security of the communication protocols was not nearly the priority that efficiency and ease of use were to developers of this technology. Things have progressed in recent years, but you have to be careful with wireless technology and be sure you have implemented encryption of the transmissions.

Section 4.1.1 of the PCC DSS specifically states, "For wireless networks transmitting cardholder data, encrypt the transmissions by using WiFi Protected Access (WPA or WPA2) technology, IPSec, Virtual Private Network (VPN), or SSL/TLS. Never rely on Wired Equivalent Privacy (WEP) to protect confidentiality and access to a wireless local area network (LAN)."

Defining WiFi

WiFi refers to particular types of wireless local area networks (WLANs), which utilize any of the 802.11 specifications of the Institute of Electrical and Electronics Engineers (IEEE). This covers pretty much any kind of modern wireless router, including ones designed for small office/home office (SOHO) use.

WPA and WPA2

Earlier versions of the 802.11 specifications for wireless communications used a technology know as WEP, which was found to be woefully inadequate as its encryption scheme was easily broken, and intercepting transmissions was a fairly trivial exercise for experienced hackers. WPA and WPA2 have both been implemented in versions of the 802.11 standards of 802.11i and beyond. WPA makes use of improved encryption standards and authentication methods. WPE should not be utilized, even though PCI DSS provides a list of compensation controls that should be utilized if it is employed.

IPSEC VPNs

IPsec is technically not just a protocol, but a framework or set of security protocols that operate at the Network layer of the Open Systems Interconnection (OSI) model. What this means in basic terms is that IPSec operates at the level of the network where devices that manage the destination of packets (like routers) operate. Accordingly, IPsec is well suited for securing the communication over a VPN.

A VPN can be described as a network that uses public infrastructure (like the Internet) to create a connection between a remote host or network to an organization's main or home network. This is a much less expensive proposition than using dedicated leased lines to provide this kind of privacy. The way a VPN works is to set up a private "tunnel" using certain protocols, which causes the data to be encrypted at the sending end and decrypted at the receiving end. It can be configured in different ways, but typically involves the installation of connection software on the client, which establishes the secure tunnel to the home network, and network devices on the home network end to serve as the secure gateway.

Another option for VPN is SSL VPN. The main advantage of an SSL VPN solution is that it does not require any additional or specialized software package on the client end. A modern standard Web browser is all that is needed, which utilizes a small plug-in to the browser to configure it.

GSM and GPRS

GSM refers to the communication system that is utilized to support mobile phone networks. GPRS is a wireless communication service that provides connection to the Internet for data transfer for mobile phones and computers. Where this might affect a wireless network and transmission of card data, would be the circumstances of utilizing a GSM/GPRS modem card in a laptop for connection to the Internet. If the requirements for implementation of the VPN and wireless protocols have been observed, it will satisfy issues related to these cards as well.

Tools & Traps…

TJX Data Theft Due to Insecure Wireless Encryption

In January of 2007, TJX Companies, which is the owner of several retails stores including TJ Maxx and Marshalls, reported a very large data breach of customer credit and debit card numbers that occurred between 2005 and 2007. TJX reported the theft of at least 45.6 million credit card numbers. Attackers were able to steal the data through an insecure wireless network at a Marshalls store in Minnesota. The Marshalls store's wireless network, which connected their credit card processing hardware to the company's back-end systems, was not protected with WPA encryption, but rather was still using the unsafe and outmoded WPE standard. Despite the fact that the WPA standard was introduced in 2002, and TJX had their backend systems protected, this vulnerability led to what is at this time the largest know breach of credit card data in history, given TJX a very dubious distinction.

Using Compensating Controls

The PCI DSS indicates that when you are unable to render cardholder data unreadable (encrypted) "due to business or technical constraints," you may consider utilizing compensating controls to achieve compliance. Implementing such compensating controls as an alternative to encryption is no small task, however. The amount of planning and management that it will involve can end up being more costly than the investment and work of encryption. You should do a very careful cost/benefit analysis

before you decide that attempting to implement the compensating controls listed in Appendix B of the PCI DSS is the way you want to go.

At a very general infosec level, a compensating control can be thought of as an internal control (which can be technical or procedural), which reduces the risk of a potential or existing vulnerability or weakness.

In terms of specific PCI context, this means making sure that locations and databases that are storing cardholder data, are segmented or protected from an organizations other systems by creating a perimeter around that stored data.

The PCI DSS requirement, which is spelled out in Section 3.4.1, however, refers us to Appendix B, which details the following specific requirements which must be met if compensation controls are utilized instead of encryption:

Compensating Controls for Requirement 3.4

"Compensating controls may consist of either a device or combination of devices, applications, and controls that meet all of the following conditions:

- Provide additional segmentation/abstraction (e.g., at the network layer)
- Provide ability to restrict access to cardholder data or databases based on the following criteria:
  - Internet Protocol (IP) address/Media Access Control (MAC) address
  - Application/service
  - User accounts/groups
  - Data type (packet filtering)
- Restrict logical access to the database
  - Control logical access to the database independent of Active Directory or Lightweight Directory Access Protocol (LDAP)
  - Prevent/detect common application or database attacks (e.g., Structured Query Language [SQL] injection)

Let's break this down a bit and discuss what each of these mean and how you might approach implementation.

Provide Additional Segmentation/ Abstraction (e.g., at the Network Layer)

Remember that the key objective is to restrict the access to systems that house cardholder data to only those users and systems that require it.

Segmentation

Segmentation essentially means separating, putting more things in front of those systems. Putting the cardholder data systems in a separate subnet segregated from other parts of the network, is the kind of action that you could take.

Abstraction

Abstraction of data refers to the process of distilling data down to its essentials. In the PCI context, implementation of this would again be to pursue putting more layers in front of the data. A database, for example, could be set up to only have access through another piece of software that queries it, in which case, you could also put logical controls on who can utilize the software making the queries to the database.

Provide Ability to Restrict Access to Cardholder Data or Databases

IP Address/Mac Address

Restricting access based on the IP address or MAC address would involve a network-level device such as a firewall. Systems that need access to a database are identified and included in an Access Control List (ACL), which allows them access. Restricting by IP address can be more difficult when utilizing Dynamic Host Control Protocol (DHCP), where the host IP changes versus the static IP addresses.

Another approach could be to utilize Network Access Control (NAC) methods. NAC technology exists in both hardware and software forms. It is a method where the NAC control sits in front of the subnet you are protecting. Security controls can be enforced and multiple checks for security requirements can be made. If the end point seeking admission to the subnet does not meet the requirement, it is denied access.

Application/Service

The implementation methods referenced in the previous section can also be utilized to restrict access to specific applications or services. Care should be taken here; methods targeted at such a low level can often backfire. Restricting based on a port that an application uses or a services, ends up causing some other application or service to fail which was not comprehended. A thorough researching of details should be made so as to not impact existing operational and network activities.

Data Type (Packet Filtering)

Packet filtering is a network-level activity, typically the work of a firewall. It is the process of dropping or allowing packets based on what the packet header says about its destination, source, its targeted port, or the protocol being used. Again, great care needs to be taken when working on this level. Some things can be identified easily as dangerous or unwanted, but simply "dropping" certain packets can often lead to applications not working, and it being difficult to determine the cause of the issue until someone thinks to examine firewall logs.

User Accounts/Groups

Even if your organization has the most fundamental information assurance program, it is likely that thought has been given to the organization of varying privileges and access based on user accounts and the groups they belong in. All operating systems and databases have the capability to restrict or allow users based on accounts and groups. This is a matter of designing the architecture, documenting it, and implementing it. Any good information assurance program starts with creating rules for access, procedures to demonstrate need for access, and implementation of auditing around when it is granted and when access is removed. No entity should have access to cardholder data without an express need for it.

Restrict Logical Access to the Database

Control Logical Access to the Database Independent of Active Directory or LDAP

This particular requirement is a bit difficult to achieve. It is essentially implying that any *centralized* directory for user groups and control is untrustworthy. This may or may not be the case in your environment, but the requirement pushes you in the direction of managing access locally. Most enterprise networks are designed to cen-

trally manage accounts, and to grant access to resources based on domain accounts. Therefore it would entail a good deal of process work regarding procedures, documentation, and process to enforce management of accounts locally on the database server or on a dedicated (segmented) Active Directory. Care must also be taken to ensure that the local accounts comply with your own corporate requirements for password compliance as well as with the PCI DSS.

Prevent/Detect Common Application or Database Attacks

The most likely candidate for a technical solution for this requirement is a network-based or host-based Intrusion Prevention System (IPS). This may be technology you already have invested in for your network, as the technology is of benefit for protection and detection of all manner of threats on the network.

IPSes monitor network traffic and take actions according to predefined rules if the traffic activity it sees meets criteria that it deems to be malicious. Many organizations also employ security event management tools. This type of technology gathers information regarding activity on the network from various sources such as event logs, firewalls, IPSes, and Intrusion Detection Systems (IDSes), and aggregates the data to detect suspicious or harmful activity on the network. The operative word in most of these technologies and approaches is *prevention*. As it relates to *detection* of attacks, this also assumes that in addition to technology that detects activity (such as IDS and AntiVirus) that procedures are in place where logs are reviewed so that it can be determined if attempts at compromise have taken place.

Overview

The primary requirement in PCI DSS regarding cardholder data is to render the data unreadable. While encryption of data on your network may be expensive, or in some cases technically impractical, it should be pursued if at all possible. The alternative measures required to meet the standards in the form of compensating controls are not trivial to achieve. They essentially require you to put into place a significant amount of internal controls and additional layers of separation from the databases that house cardholder data. Implementing and maintaining the hardware, software, policies, and procedures necessary for this additional internal perimeter could become an odious task. Without great care in implementation, you could still end up not passing a PCI audit, and in the process could break necessary internal data flows, which are required for your processes to work.

Mapping Out a Strategy

Now that we've looked at the particulars of the PCI requirements for protecting cardholder data, and discussed some of the technologies and methods available to achieve compliance, let's take a step back and briefly discuss your approach.

In many cases, organizations involved in handling PCI data existed and were involved with it before the PCI DSS came out. So, networks and architecture processes already existed. If you were designing your network and your plan from the ground up with PCI DSS in mind, you'd do it differently. Attempting to apply specific security standards after the fact is a different (and more difficult) proposition.

By utilizing some of the fundamental principles of developing a sound information management practice, you can avoid a haphazard approach that can lead to problems such as inefficiency, unnecessary cost, insufficient controls, or controls that are more restrictive than necessary.

Step 1—Identify and Classify Information

The first step in achieving your data privacy goals is to identify what data you have and classify it in terms of its sensitivity. There are multiple levels that data can be classified on, but for the purposes of PCI, you need to determine what is and is not cardholder data, and then break down the elements further in terms of sensitivity. You might break it down such as:

- Customer Information
- PAN
- Personal Identification Number (PIN) number
- Non-customer-related data

You can classify your data in any way that makes sense to you, but the most important thing to be aware of is the requirements in PCI DSS Requirement 3 in terms of what is required to be treated as sensitive or not. Your subsequent steps of organization will be based on your decisions here.

Step 2—Identify Where the Sensitive Data is Located

Databases will house cardholder data, but where else might it be? Flat files that are results of batch processing, log files, backup tapes, and storage networks may all house sensitive information.

Ask the following questions:

- Where is it located?
- What format is it in (e.g., database, flat file)?
- What is the size of the data?

Answers to these questions will determine if you have to make changes in your architecture to minimize the cost and work to protect the data.

Step 3—Determine Who and What Needs Access

Too often, data breaches take place simply because people and applications have access to data they do not need. You have to balance the need for access with the proper control on that access to keep doing business.

Answer these questions:

- Who currently has access to sensitive data?
- Do they need access to do their job?
- What format is it in (e.g., database, flat file)?
- What is the size of the data?
- What applications such as backup applications or Web sites need access?

Step 4—Develop Policies Based On What You Have Identified

Now that you have identified what data you have, where your data is located, and who and what needs to access it, you can define information-handling policies based on what, where, who, and how. This is where you establish such things as policies, standards, guidelines, and procedures. The details of implementing this are beyond the scope of this book, but numerous resources exist which provide help on how to

approach this in an organized way. It may also be of help for you to engage a professional organization or consultant versed in this to help you write and publish these. This will be the cornerstone of your approach to your information assurance plan.

The Absolute Essentials

We've approached the protection of the cardholder data from PCC DSS from a high-level, principle-driven approach. The PCI data security standards are published and available, and you need to be familiar with them in detail to insure you are compliant.

Let's take a moment to review what would be considered the absolutes detailed in Requirement 3.

Keep Cardholder Storage to a Minimum

As part of your development of policies, you will establish a data retention policy. This is a crucial piece of an information assurance plan. There is no need to store sensitive data longer than business, legal, and regulatory requirements dictate.

Do Not Store Sensitive Authentication Data Subsequent to Authorization

Once a transaction has been authorized or "cleared," there is no justification for storing any of the following sensitive data:

- Full contents of any track from the magnetic stripe on the back of the card
- Card verification code
- PIN
- PIN block (encrypted pin block)

Mask the PAN When Displayed

The first six digits and the last four digits are the *maximum* that can be displayed. (Point of Sale restriction may be more demanding that this standard.) This is focused on the storage, retrieval, and display of the number.

Render PAN (at Minimum) Unreadable Anywhere it is Stored

This requirement is most easily achieved by encryption. But other methods are allowed, such as a one-way hash, truncating, and padding.

Protect Encryption Keys Used for Encryption of Cardholder Data Against Both Disclosure and Misuse

PCI DSS details 12 different items for the proper management of encryption keys. These will not be detailed here other than to point out that this is again something that would be included in your policies. They include processes, procedures, and who the custodian of these keys would be. The management of encryption keys is probably the most resource-intensive aspect of encryption. Some methods of encryption make this simpler than others. Consider this aspect and make sure you ask the right questions of potential vendors when considering your encryption solution(s).

Summary

Complying with the PCI DSS requirements is not a trivial task. Many organizations are still not compliant and risk fines and data breaches as a consequence. With the proper preparation and execution of your plan, you can protect the information you have been entrusted with. Keep these key components in mind:

- Identify where the sensitive data is on the network, and establish sound policies for handling it based on that identification.
- Securing data at rest can involve encryption or compensating controls, but attempting to segregate sensitive cardholder data by logical and physical controls only can be very tricky.
- Securing data in-transit is important to your organization, regardless of the business you are in. As it relates to PCI standards, it is crucial. When sending data over an open, public network, the data stream must be secured or you risk exposing cardholder data to attackers. One single instance of failure could be the point where you are exploited, such as a wireless router utilizing old and exploitable encryption.
- The place to start to protect yourself and your data is to ensure that you do not store any sensitive cardholder data after a transaction has been authorized. It is not necessary.

Solutions Fast Track

Protecting Data at Rest

- ☑ The most sure way of protecting sensitive cardholder data stored on your network is by using encryption.
- ☑ Multiple methods for encryption exist including file- or folder-level encryption, full disk encryption, and database (column-level) encryption. Each have their own advantages and disadvantages
- ☑ If encryption is not an option, specific compensating controls can me implemented, but they are not trivial to employ.

Protecting Data in Transit

- ☑ When cardholder data is transmitted across an open, public network, it must be encrypted.
- ☑ IPSec VPN technology is a common way to establish a secure "tunnel" between trusted networks.
- ☑ Web servers and e-mail servers need to be configured to utilize secure communication protocols when transmitting cardholder data.
- ☑ WiFi network devices need to be secured by current, secure encryption protocols, such as WPA or WPA2.

Compensating Controls

- ☑ If an organization cannot utilize encryption to render cardholder data unreadable, it is allowable to utilize compensation controls to provide segregation of the sensitive data.
- ☑ Putting a perimeter around storage locations that house sensitive data, can be achieved through various methods of segmentation and abstraction as defined by PCI DSS.
- ☑ The ability to restrict access to locations and databases that house cardholder data, must be provided. This can be done on various levels, including restricting access-based IP or MAC addresses, applications or services, data types, users, or accounts.
- ☑ Logical access to databases that house cardholder data must be implemented independent of Active Directory or LDAP groups and accounts.

Starting With a Strategy

- ☑ Identifying and classifying the data on your network in terms of its sensitivity, is the first step in mapping out your plan of attack for securing it.
- ☑ Once you have identified the data types you have, identifying where it is located and what form it is in follows.
- ☑ You need to determine what people and what applications need access to your data to fulfill your organization's business requirements.

- ☑ Having established the who, what, and where of your data, you can then develop roles, polices, procedures, and guidelines to manage that data and ensure you have consistent practices

The Absolute Essentials

- ☑ Storage of cardholder data needs to be kept to the absolute minimum required to do business.
- ☑ Sensitive cardholder authentication data is not to be stored after authorization has taken place.
- ☑ The PAN should be masked whenever it is displayed.
- ☑ The PAN (at the very minimum) needs to be rendered unreadable wherever it is stored. This can be accomplished by encryption, one-way hashes, and other methods.
- ☑ PCI DSS outlines several specific requirements for how encryption keys used for encryption of cardholder data must be managed.

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to **www.syngress.com/solutions** and click on the **"Ask the Author"** form.

Q: What happens when I have my environment assessed for compliance?

A: An audit for PCI DSS compliance is very similar to other kinds of process audits. Make sure you have your processes and procedures documented. An assessor would check your environment to make sure that you follow the procedures you have documented, and that sensitive data is being secured properly.

Q: Is there any way to prepare for assessment and make sure I've covered everything?

A: In addition to being thoroughly familiar with the PCI DSS documentation, the PCI Security Standards Council also provides a handy Self Assessment Questionnaire to assist organizations in their overall review of the environment. It

can be downloaded from https://www.pcisecuritystandards.org/pdfs/pci_saq_v1-0.pdf.

Q: Are problems with PCI DSS Requirements 3 and 4 a common cause of PCI standards compliance failures?

A: Yes, failure to properly secure sensitive data at rest, and failure to properly encrypt and secure it during transmission, are the most common sources of failure in compliance to PCI DSS standards. In November of 2006, Visa USA Cardholder Information Security Program (CISP) issued a bulletin which underscored this fact, specifically focusing on improperly installed and maintained point-of-sale (POS) systems.

Q: What are the "low hanging fruit" issues I can take care of first to secure sensitive data?

A: Take care of any and all access to data from the outside. There should be no direct access to a POS system. Ensure that wireless routers are secured and configured properly. Remove remote access software that employees may have installed to make work convenient.

Q: How do I make sure that the secure configuration I put into place stays that way?

A: It is wise to utilize come kind of "configuration management" software solution such as Tripwire, if possible. You can configure such software to alert you to, or generate reports on, changes in configuration of accounts, files, and logs. You can even configure it to force changes back to the original version, if desired. This can be time consuming to implement, but can protect you from unexpected and unwanted changes that threaten the security of your environment.

Chapter 6

Logging Access & Events Chapter

Solutions in this chapter:

- **Introduction to Logging In PCI Requirement 10**
- **Logging in PCI – All Other Requirements**
- **Tools for Logging in PCI**

- ☑ **Summary**
- ☑ **Solutions Fast Track**
- ☑ **Frequently Asked Questions**

Introduction to Logging

System and network logs are often called the "untapped riches." The now-famous humorous security calendar proclaims "Logs: Let'em Rot." Others just quietly choose to follow this maxim and ignore logs—at their own peril—altogether.

On the other hand, as computer and Internet technology continues to spread and computers start playing an even more important role in our lives, the records that they produce, a.k.a. logs, start to play a bigger role. From firewalls and x to databases and enterprise applications, to wireless access points and Voice over Internet Protocol (VoIP) gateways, logs are being spewed forth at an ever-increasing pace. Both security and other Information Technology (IT) components not only increase in numbers, but also often come with more logging enabled out of the box. An example of this trend includes Linux systems and Web servers that now ship with increased levels of logging. All those systems, both legacy and modern, are known to generate copious amounts of logs, audit trails, records, and alerts, that beg for constant attention.

But this is easier said than done. Immense volumes of log data are being generated on payment card processing networks, necessitating more efficient ways of managing, storing, and searching through log data, both reactively—after a suspected incident—and proactively—in search of potential risks. For example, a typical retailer generates hundreds of thousands of log messages per day amounting to many terabytes per year. An online merchant can generate upwards of 500,000 log messages every day. One of America's largest retailers has more than 60 terabytes of log data on their systems at any given time. Unlike other companies, retailers often do not have the option of not using logging.

NOTE

Even though we refer to "retailers," Payment Card Industry (PCI) is not only about retailers, but pretty much everybody who touches credit card numbers in the course of their business.

To start our discussion of PCI logging requirements and to define the context, Table 6.1 below contains a sample list of technologies that produce logs. Though this list is not comprehensive, it is likely that the reader will find at least one system that they have in their environment and for which logs are not being collected, much less looked at.

Table 6.1 Log-Producing Technologies

Type	Examples
Operating Systems	Linux, Solaris, Windows
Databases	Oracle, SQL Server
Network infrastructure	Cisco routers and switches
Remote access	Internet Protocol Security (IPSec), Virtual Private Networks (VPNs), and Secure Socket Layer (SSL) VPNs
Network security	Checkpoint FireWall-1, Cisco PIX firewalls
Intrusion detection and preventions	Snort NIDS, ISS RealSecure
Enterprise applications	SAP, PeopleSoft
Web servers	Apache, Internet Information Server (IIS)
Proxy servers	BlueCoat, Squid
E-mail servers	Sendmail, Exchange
DNS servers	ISC Domain name system (DNS), MS DNS
Anti-virus and anti-spyware	Symantec AV, TrendMicro AV
Physical access control	IDenticard, CoreStreet
Wireless networking	Cisco Aironet AP, Netgear AP

NOTE

Table 6.1 is not a full list; everybody will have some esoteric and not so esoteric applications and devices that produce logs that are not covered in this table. In any case, if these devices are included in a payment card environment, it is likely that these device logs will need to be collected, stored, and analyzed to satisfy PCI Requirement 10 as well as others.

Many companies and government agencies are trying to set up repeatable log collection, centralization, and analysis processes and tools.

Despite the multitude of log sources and types, people typically start from network and firewall logs and then progress upward on the protocol stack as well as sideways towards other non-network applications. For example, just about any firewall or network administrator will look at a simple summary of connections that his

Private Internet Exchange (PIX) or Checkpoint is logging. Many firewalls log in standard syslog format and such logs are easy to collect and review.

Reviewing network Intrusion Detection System (IDS) logs (for those companies that chose to deploy this technology), while "interesting" in case of an incident, is often a very frustrating task since Network Intrusion Detection Systems (NIDSes) would sometimes produce "false alarms" and dutifully log them. Still, NIDS log analysis, at least the post-mortem kind for investigative purposes, often happens right after firewalls when organizations deploy their log management infrastructure for compliance, security, or operational uses since the value of such info for security is undeniable and logs can, in most cases, be easily centralized for analysis.

Even though system administrators always knew to look at logs in case of problems, massive server operating system (both Windows and UNIX/Linux variants) log analysis didn't materialize until more recently. Collecting logs from Windows servers, for example, was hindered by the lack of agentless log collection tools, such as LASSO, that only emerged in the last year or two. On the other hand, UNIX server log analysis was severely undercut by a total lack of unified format for log content in syslog records.

Web server logs were long analyzed by marketing departments to check on their online campaign successes. Most Web server administrators would also not ignore those logs. However, since Web servers don't have native log forwarding capabilities (most log to files stored on the server itself), consistent centralized Web log analysis for both security and other IT purposes is still ramping up.

Tools and Traps

The Apache Web server has a few types of logs. The most typical among them are *access_log* that contains all page requests made to the server (with their response codes), and *error_log* that contains various errors and problems. Other Apache logs relate to Secure Sockets Layer (SSL) (*ssl_error_log*) as well as optional granular audit logs that can be configured using tools such as ModSecurity (*audit_log*)

Similarly, e-mail tracking through e-mail server logs languishes in a somewhat similar manner: people only turn to e-mail logs when something goes wrong (e-mail failures) or horribly wrong (external party subpoenas your logs). Lack of native centralization and, to some extent, complicated log formats slowed down the e-mail log analysis initiatives.

Even more than e-mail, database logging wasn't on the radar of most Information Technology (IT) folks until last year. In fact, IT folks were perfectly happy with the

fact that even though Relational Database Management Systems (RDBMSes) had extensive logging and data access auditing capabilities, most of them were never turned on. Oracle, Microsoft Structured Query Language (SQL) Server, IBM DB2, and MySQL all provide excellent logging, if you know how to enable it, configure it for your specific needs, and analyze and leverage the resulting onslaught of data.

What's next? Web applications and large enterprise application frameworks largely lived in a world of their own, but now people are starting to realize that their log data provides unique insight into insider attacks, insider data theft, and other trusted access abuse. Additionally, desktop operating system log analysis from large numbers of deployed desktops will also follow.

PCI Relevance of Logs

Which logs are relevant to your PCI project? In some circumstances, the answer is "all of them," but it is more likely that logs from systems that handle credit card information (as well as systems that connect to, protect, or otherwise relate to such systems) will be in scope. PCI Data Security Standard (DSS) requirements apply to all members, merchants, and service providers that store, process, or transmit cardholder data. Additionally, these requirements apply to all "system components," which is defined as "any network component, server, or application included in, or connected to, the cardholder data environment." Network components include, but are not limited to, firewalls, switches, routers, wireless access points, network appliances, and other security appliances. Servers include, but are not limited to, Web, database, authentication, Domain name system (DNS), e-mail, proxy, and Network Time Protocol (NTP) servers. Applications include all off-the-shelf and custom-built applications, including internally facing and externally facing Web applications.

The following are a few common uses for log information, besides for PCI compliance:

- **Threat Detection** Historical Host Intrusion Detection Systems (HIDSes) from the 1990s looked at audit trails and logs in search of patterns and strings in logs, and raised alerts upon seeing them. Today, hunting for signs of hacking attempts (as well as successes in the form of "compromise detection") in logs is just as useful.
- **Incident Response and Troubleshooting** When a system is hacked, logs are the most informative, accessible and relatively easy to analyze (compared to full disk images) form of incident evidence.

- **Audit** IT auditors as well as PCI assessors commonly ask for logs from in-scope systems.
- **E-discovery** While some say that a possibility of a subpoena or an e-discovery requests provides a compelling reason to not have logs, in reality, hiding one's head in the sand is unlikely to work in this case.
- **IT Performance Management and Troubleshooting** Network is slow? Looking at logs will help find out why.
- **Network Management** While log pundits might argue on whether a Simple Network Management Protocol (SNMP) trap is a kind of log record, logs are useful for many bandwidth management and network performance measurement tasks that are common in IT.
- **Compliance** Just about every recent regulatory compliance or "best practices" framework touches on audit logs

Now we are ready to dive into the specifics of PCI and logging.

Logging in PCI Requirement 10

Let's quickly go through Requirement 10, which directly addresses logging. We will go through it line by line and go into details, examples, and implementation guidance later in this chapter.

The requirement itself is called Track, and monitors all access to network resources and cardholder data and is organized under the "Regularly Monitor and Test Networks" heading. Thus it deals with both periodic (test) and ongoing (monitor) aspects of maintaining your security. More specifically, it requires a network operator to track and monitor all access to network resources and cardholder data. Thus, both network resources that handle the data and the data itself are subject to those protections.

Further, the requirement states that logging is critical, primarily when "something does go wrong" and one needs to "determine the cause of a compromise" or other problem. Indeed, logs are of immense importance for incident response. However, using logs for routine user tracking and system analysis cannot be underestimated.

Next, the requirement is organized in several sections on process, events that need to be logged, suggested level of details, time synchronization, audit log security, required log review, and log retention policy.

Specifically, Requirement 10.1 covers "establish[ing] a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user." This is a very interesting requirement indeed; it doesn't just mandate for logs to be there or for a logging process to be set, but instead mentions that logs must be tied to individual persons (not computers or "devices" where they are produced). It is this requirement that often creates problems for PCI implementers, since many think of logs as "records of people actions," while in reality they will only have the "records of computer actions." Mapping the latter to actual flesh-and-blood users often presents an additional challenge.

Next, Section 10.2 defines a minimum list of system events to be logged (or, to allow "the events to be reconstructed"). Such requirements are motivated by the need to audit and monitor user actions as well as other events that can affect credit card data (such as system failures)

NOTE

It is hoped that in the future such a list of system events will be determined by the overall log standards that go beyond PCI. There are ongoing log standard projects that have a chance to produce such a universally accepted (or at least, industry-accepted) list of events in the next 2 to 3 years.

Following is the list from the requirements (events that must be logged):

- 10.2.1 All individual user accesses to cardholder data
- 10.2.2 All actions taken by any individual with root or administrative privileges
- 10.2.3 Access to all audit trails
- 10.2.4 Invalid logical access attempts
- 10.2 5 Use of identification and authentication mechanisms
- 10.2.6 Initialization of the audit logs
- 10.2.7 Creation and deletion of system-level objects

As can be seen, this covers data access, privileged user actions, log access and initialization, failed and invalid access attempts, authentication and authorization decisions, and system object changes. It is important to note that such a list has its roots

in IT governance "best practices," which prescribe monitoring access, authentication, authorization (AAA), change management, system availability, and suspicious activity. Thus, other regulations, such as the Sarbanes-Oxley Act and IT governance frameworks such as COBIT, have very similar lists of events that need to be logged.

Moreover, PCI DSS Requirement 10 goes into an even deeper level of detail and covers specific data fields or values that need to be logged for each event. They provide a healthy minimum requirement, which is commonly exceeded by logging mechanisms in various IT platforms.

Such fields are:

- 10.3.1 User identification
- 10.3.2 Type of event
- 10.3.3 Date and time
- 10.3.4 Success or failure indication
- 10.3.5 Origination of event
- 10.3.6 Identity or name of affected data, system component, or resource

As can be seen, this minimum list contains all of the basic attributes needed for incident analysis and for answering the questions: when, who, where, what, and where from. For example, if you are trying to discover who modified a credit card database to copy all of the transactions with all the details into a hidden file (a typical insider privilege abuse), you would need to know all of the above. Table 6.2 summarizes the above fields in this case.

Table 6.2 PCI Event Details

PCI Requirement	Purpose
10.3.1 User identification	Which user account is associated with the event being logged? This might not necessarily mean "which person," only which username.
10.3.2 Type of event	Was it a system configuration change? File addition? Database configuration change? Explains what exactly happened.
10.3.3 Date and time	When did it happen? This information helps in tying the event to an actual person

Continued

Table 6.2 continued PCI Event Details

PCI Requirement	Purpose
10.3.4 Success or failure indication	Did he or she try to do something else that failed before his or her success in changing the configuration?
10.3.5 Origination of event	Where did he or she connect from? Was it a local access or network access? This also helps in tying the log event to a person. Note that this can also refer to the process or application that originated the event.
10.3.6 Identity or name of affected data, system component, or resource	What is the name of database, system object, and so forth which was affected? Which server did it happen on? This provides important additional information about the event.

The next requirement, 10.4, addresses a commonly overlooked but critical requirement: a need to have accurate and consistent time in all of the logs. A need to "synchronize all critical system clocks and times" can make or break your incident response, or lead to countless hours spent figuring out the actual times of events by correlating multiple sources of information together. In some cases, uncertainty about the log timestamps might even lead a court case to be dismissed, because uncertainly about timestamps might lead to uncertainty in other claims as well. For example, from "so you are saying you are not sure when exactly it happened?" an expert attorney might jump to "so maybe you are not even sure what happened?" Fortunately, this requirement is relatively straightforward to address by configuring an NTP environment and then configuring all servers to synchronize time with it. The primary NTP servers can synchronize time with *time.nist.gov* or other official time sources.

Security of the logs themselves is of paramount importance for reasons similar to the above concerns about the log time synchronization. Requirement 10.5 states that one needs to "secure audit trails so they cannot be altered" and then clarifies various risks that needs to be addressed.

Are You Owned

While PCI is more about being compliant than about being owned (or, rather, not owned), logs certainly help to answer this question. However, if logs themselves are "owned" and the log server is compromised, they lose all value for either security or

compliance purposes. Thus, having assured log confidentiality, integrity, and availability is a requirement for PCI as well as a best practice for other log uses.

First, one needs to address all of the confidentiality, integrity and availability (CIA) of logs. Section 10.5.1 covers the confidentiality: "Limit viewing of audit trails to those with a job-related need." This means that only those who need to see the logs to accomplish their jobs should be able to. What is so sensitive about logs? One of the obvious reasons is that authentication-related logs will always contains usernames. While not truly secret, username information provides 50 percent of the information needed for password guessing (password being the other 50 percent) Why give possible attackers (whether internal or external) this information? Moreover, due to users mistyping their credentials, it is not uncommon for passwords themselves to show up in logs. Poorly written Web applications might result in a password being logged together with the Web Uniform Resource Locator (URL) in Web server logs. For example, a UNIX server log might contain a user password if the user accidentally presses "Enter" one extra time while logging in.

Second, as 10.5.2 states, one needs to "protect audit trail files from unauthorized modifications." This one is blatantly obvious, since if logs can be modified by unauthorized parties (or by anybody) they stop being an objective audit trail of system and user activities.

However, one needs to preserve the logs not only from malicious users, but also from system failures and consequences of system configuration errors. Specifically, Section 10.5.3 covers that one needs to "promptly back-up audit trail files to a centralized log server or media that is difficult to alter." Indeed, centralizing logs to a server or a set of servers that can be used for log analysis is essential for both log protection as well as increasing log usefulness. Backing up logs to CDs or DVDs (or tapes) is another consequence of this requirement. One should always keep in mind that logs on tape are not easily accessible and not searchable in case of an incident.

Many pieces of network infrastructure such as routers and switches are designed to log to an external server and only preserve a minimum (or none) of logs on the device itself. Thus, for those systems, centralizing logs is most critical. Requirement 10.5.4 states the need to "copy logs for wireless networks onto a log server on the internal LAN."

To further decrease the risk of log alteration as well as to enable proof that such alteration didn't take place, Requirement 10.5.5 calls for the "use file integrity monitoring and change detection software on logs to ensure that existing log data cannot be changed without generating alerts." At the same time, adding new log data to a

log file should not generate an alert since log files tend to grow and not shrink on their own (unless logs are rotated or archived to external storage) File integrity monitoring systems use cryptographic hashing algorithms to compare files to a known good copy. The issues with logs is that log files tend to grow due to new record addition, thus undermining the missing of integrity checking. To resolve this contradiction, one should note that integrity monitoring can only assure the integrity of logs that are not being actively written to by the logging components.

The next requirement is truly one of the most important as well as one of the most often overlooked. Many PCI implementers simply forget that PCI Requirement 10 does not just call for "having logs," but also for "having the logs AND looking at them." Specifically, Section 10.6 states that the PCI organization must "review logs for all system components *at least daily*. Log reviews must include those servers that perform security functions like IDSes and AAA servers (e.g., RADIUS)."

Thus the requirement covers the scope of log sources that need to be "reviewed daily" and not just configured to log, and have logs preserved or centralized. Given that a Fortune 1000 IT environment might produce gigabytes of logs per day, it is humanly impossible to read all of the logs. That is why a note is added to this requirement that states that "Log harvesting, parsing, and alerting tools may be used to achieve compliance with Requirement 10.6." Indeed, log management tools are the only way to go in order to satisfy this requirement.

The final requirement (10.7) deals with another hugely important logging question—log retention. It says: "retain audit trail history for at least one year, with a minimum of three months online availability." Unlike countless other requirements, this deals with the complicated log retention question directly. Thus, if you are not able to go back one year and look at the logs, you are in violation. Moreover, PCI DSS in its updated version v1.1 got more prescriptive when a one-year requirement was added explicitly.

So, let us summarize what we learned so far on logging in PCI:

- PCI Requirement 10 calls for logging specific events with a pre-defined level of details from all in-scope systems
- PCI calls for tying the actual users to all logged actions
- All clocks and time on the in-scope systems should be synchronized
- The CIA of all collected logs should be protected

- Logs should be regularly reviewed; specific logs should be reviewed at least daily
- All in-scope logs should be retained for at least one year

Now we are ready to dig deeper to discover that logs "live" not only within Requirement 10, but in all other PCI requirements.

Logging in PCI – All Other Requirements

While many think that logs in PCI are represented only by Requirement 10, reality is more complicated: logs are in fact present, undercover, in all other sections. We will now reveal where they hide in other sections. Table 6.3 highlights some of the places where logging requirements are implied or mentioned. The overall theme here is that logging and log management assists with validation and verification of many other requirements.

Table 6.3 Logging in Other PCI Requirements

#	Area	Requirement	Logging Relevance and Recommendations
1	**Build and Maintain a Secure Network**	Install and maintain a firewall configuration to protect cardholder data	Enable firewall logging; review logs for access violations, use of risky protocols, device configuration changes, accesses to critical network segments.
2	**Build and Maintain a Secure Network**	Do not use vendor-supplied defaults for system passwords and other security parameters	Review logs to look for insecure services, additional services starting on servers, as well as password changes upon server deployment.
3	**Protect Cardholder Data**	Protect stored cardholder data	Review the logs related to key management to verify that the requirements (such as key changes, and so forth) are being followed.

Continued

Table 6.3 continued Logging in Other PCI Requirements

#	Area	Requirement	Logging Relevance and Recommendations
4	**Protect Cardholder Data**	Encrypt transmission of cardholder data across open, public networks	Look at firewall, Virtual Private Network (VPN) logs to verify that only secure network communication is used.
5	**Maintain a Vulnerability Management Program**	Use and regularly update anti-virus software	Verify that anti-virus software is updated by looking at anti-virus logs; also look for detection and mitigation failures that might indicate that malware is present on the network.
6	**Maintain a Vulnerability Management Program**	Develop and maintain secure systems and applications	Make sure that custom applications written or customized for your environment also provide logging. Watch logs of system update and software distribution servers to make sure patches are being deployed when needed on all relevant servers.
7	**Implement Strong Access Control Measures**	Restrict access to cardholder data by business need-to-know	Verify that such access is indeed limited by reviewing the access logs.
8	**Implement Strong Access Control Measures**	Assign a unique ID to each person with computer access	Perform log correlation to detect ID sharing in violation of this requirement; review logs indicating changes to users' privileges; verify password changes based on authentication systems logs, and so forth.

Continued

Table 6.3 continued Logging in Other PCI Requirements

#	Area	Requirement	Logging Relevance and Recommendations
			Look for administrator and root accounts that can sometimes be shared (and are rarely removed from systems).
9	**Implement Strong Access Control Measures**	Restrict physical access to cardholder data	Collect, analyze and review physical access control system logs.
10	**Regularly Monitor and Test Networks**	Track and monitor all access to network resources and cardholder data	Covered above.
11	**Regularly Monitor and Test Networks**	Regularly test security systems and processes	Verify that vulnerability assessment is being performed, by looking at the logs.
12	**Maintain an Information Security Policy**	Maintain a policy that addresses information security	Make sure that logs and logging are represented in your security policy as well as operational standards, procedures, and management reports.

Now, let's look at some of the above sections and dive deeper into the role of logs in order to further explain that logs are not only about the Requirement 10. Just about every claim that is made to satisfy the requirements, such as data encryption or anti-virus updates, can make effective use of log files to actually substantiate it.

For example, Requirement 1, "Install and maintain a firewall configuration to protect cardholder data" mentions that organizations must have "a formal process for approving and testing all external network connections and changes to the firewall configuration." However, after such process is established, one needs to validate that firewall configuration changes do happen with authorization and in accordance with documented change management procedures. That is where logging becomes extremely handy, since it shows you what actually happened and not just what was supposed to happen.

Specifically, seeing a message such as this Cisco ASA appliance record:

percentASA-5-502103: User priv level changed: Uname: jsmith From: privilege_level1 To: privilege_level2

should indicate that someone is likely trying to modify the appliance configuration. Or this message:

percentPIX-5-111004: 10.1.1.1 end configuration: FAILED

indicates a failure to complete configuration update.

Other log-related areas within Requirement 1 include Section 1.1.6 - Justification and documentation for any available protocols besides Hypertext Transfer Protocol (HTTP), SSL, Secure Shell (SSH), and VPN where logs should be used to watch for all event triggered due to such communication

Section 1.1.7 - Justification and documentation for any risky protocols allowed (for example, file transfer protocol [FTP], which includes the reason for use of protocol and security features implemented, where logs help to catalogue the user of "risky" protocols and then monitor such use.

The entire Requirement 1.3 contains guidance to firewall configuration, with specific statements about inbound and outbound connectivity. One must use firewall logs to verify this; even a review of configuration would not be sufficient, since only logs show "how it really happened" and not just "how it was configured."

Similarly, Requirement 2 talks about password management "best practices" as well as general security hardening, such as not running unneeded services. Logs can show when such previously disabled services are being started, either by misinformed system administrators or by attackers. For example, if Apache Web server is disabled on an e-mail server systems, a message such as:

[Sun Jul 18 04:02:09 2004] [notice] Apache/1.3.19 (Unix) (Red-Hat/Linux) mod_ssl/2.8.1 OpenSSL/0.9.6 DAV/1.0.2 PHP/4.0.4pl1 mod_perl/1.24_01 configured — resuming normal operations

should trigger an alert since the service should not be starting (or restarting).

Further, Requirement 3, which deals with data encryption, has direct and unambiguous links to logging. For example, the entire subsection 3.6, shown below in an abbreviated form, implies having logs to verify that such activity actually take place.

> **"3.6** Fully document and implement all key management processes and procedures for keys used for encryption of cardholder data, including the following:

3.6.1 Generation of strong keys

3.6.2 Secure key distribution

3.6.3 Secure key storage

3.6.4 Periodic changing of keys

3.6.5 Destruction of old keys"

and so forth.

Specifically, key generation, distribution, and revocation are logged by most encryption systems and such logs are critical for satisfying this requirement.

Requirement 4, which also deals with encryption, has logging implications for similar reasons.

Requirement 5 refers to anti-virus defenses. Of course, in order to satisfy Section 5.2, which requires that you "Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs," one needs to see such mentioned logs.

For example, Symantec Anti-Virus might produce the following record:

Product: Symantec AntiVirus — Error 1706. AntiVirus cannot continue.

which occurs when the anti-virus software experiences problems and cannot continue scanning, thus putting you in violation of PCI DSS rules. So, even the requirement to "use and regularly update anti-virus software" will likely generate requires for log data during the audit, since the information is present in anti-virus audit logs. It is also well-known that failed anti-virus updates, also reflected in logs, expose the company to malware risks, since anti-virus without the latest signature updates only creates a false sense of security and undermines the compliance effort.

Requirement 6 is in the same league: it calls for the organizations to "Develop and maintain secure systems and applications," which is unthinkable without a strong audit logging function.

Requirement 7, which states that one needs to "Restrict access to cardholder data by business need-to-know," requires logs to validate who actually had access to said data. If the users that should be prevented from seeing the data appear in the log files as accessing the data usefully, remediation is needed.

Assigning a unique ID to each user accessing the system fits with other security "best practices." In PCI it is not just a "best practice"; it is a requirement (Requirement 8 "Assign a unique ID to each person with computer access").

Obviously, one needs to "Control addition, deletion, and modification of user IDs, credentials, and other identifier Objects" (Section 8.5.1) Most systems log such activities. For example the

percentPIX-5-502101: New user added to local dbase: Uname: anilt Priv: 1 Encpass: 56Rt8U

message indicates a new user being added to a PIX firewall.

In addition, Section 8.5.9, "Change user passwords at least every 90 days," can also be verified by reviewing the logs files from the server in order to assure that all the accounts have their password changed at least every 90 days.

Requirement 9 presents a new realm of security—physical access control. Even Section 9.4 that covers maintaining a visitor logs (likely in the form of a physical log book) is connected to log management if such a visitor log is electronic. There are separate data retention requirements for such logs: "Use a visitor log to maintain a physical audit trail of visitor activity. Retain this log for a minimum of three months, unless otherwise restricted by law."

Requirement 11 addresses the need to scan (or "test") the in-scope systems for vulnerabilities However, it also calls for the use of IDS in Section 11.4: "Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines up-to-date." This has obvious implications to log management, since the above systems spew forth copious amounts of logs.

Requirement 12 covers the issues on a higher level—security policy as well as security standards and daily operational procedures (e.g., a procedure for daily log review mandates by Requirement 10 should be reflected here). However, it also has logging implications, since audit logging should be a part of every security policy. In addition, incident response requirements are also tied to logging: "Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations" is unthinkable to satisfy without effective collection and timely review of log data.

Thus, a logs value to PCI program goes much beyond Requirement 10. Only through careful log data collection and analysis can companies meet the broad requirements of PCI. Such detailed log data management requires embedded intelligence in the log management solutions to make the data secure, accessible, and easy to organize and to automate many of the required tasks, such as monitoring, analysis, and retention.

Tools for Logging in PCI

Now that we went through the entire PCI guidelines and uncovered the logs that are well represented there, we have a mammoth task ahead—how to address all those requirements? Let's quickly go back to one of the previous sections and review what we learned about logging in PCI, both in Requirement 10 and beyond.

- We need to make sure we log specific events with a pre-defined level of detail from all in-scope systems.
- PCI calls for tying the actual users to all logged actions.
- All time on the in-scope systems should be synchronized.
- The CIA of all collected logs should be protected.
- Logs should be regularly reviewed; specific logs should be reviewed at least daily. Automation of such review is not only acceptable, but desirable, since manual review is guaranteed to fail (on high-volume networks)
- All in-scope logs should be retained for at least one year.
- In-scope systems include at least all systems that directly process credit card data (such as PAN and other private cardholder information), including underlying operating systems as well as data processing applications, systems that store such data, network infrastructure for networks where such data is transmitted, and systems that protect any of the above (such as firewalls, network IDS and Internet Protocol Security [IPS]). This also includes systems not specifically segregated from these processing servers and applications.

Let's analyze the above requirements and needs in order to determine what kind of tools we might need to develop or procure.

First, let's note that if we are talking about a single server and a single piece of network gear such as a router, there might be no need for automation and tools. One can easily configure logging and then look at the logs (measuring a few pages of text a day or more, in case more comprehensive auditing is performed), as well as save a copy of said logs to make sure that one can go back a year and review the old logs if needed. However, this approach fails miserably and dramatically when the number of systems grows from 1 to, say, 10. In reality, a large e-commerce site or a whole chain of stores might easily have thousands of in-scope systems, starting from mainframes with customer databases down to servers to complex network architectures (including classic LANs, WANs, wireless networks, and remote access systems with

hundreds of remote users) to POS systems and all the way down to wireless card scanners. A handheld wireless card scanner is "a credit card processing system" and thus is in scope for PCI compliance. Looking through recent media headlines, such as credit card compromises at BestBuy and other "brick and mortar" retailers, one learns that credit card information has indeed been stolen this way.

Once it has been accepted that manual review of logs is not feasible or effective, the next attempt to satisfy the requirements usually comes in the form of scripts written by system administrators, to filter, review and centralize the logs as well as makeshift remote logging collectors (usually limited to those log sources that support syslog, which is easy to forward to another system).

For example, one might configure all in-scope Unix servers to log a single "log server" and then write a Perl script that will scan the logs for specific strings (such as "fail*," "attack," "denied," "modify," and so forth) and then send an e-mail to the administrator upon finding one of those strings. Another script might be used to summarize the log records into a simple "report" that highlights, for example, "Top Users" or "Top IP Addresses." A few creative tools were written to implement various advanced methods of log analysis, such as rule-based or stateful correlation.

Such "solutions" work well and do not require any initial investment. Other advantages of such "homegrown" approaches are:

- You are likely to get exactly what you want since you design and build the tool for your environment.
- You can develop tools that have capabilities not offered by any commercial tool vendor.
- The choice of platform, development tools, analysis methods and everything else is yours alone.
- You can later customize the solution to suit your future needs.
- There is no up-front cost for buying software and even hardware (if you are reusing some old unused servers, which is frequently the case for such log analysis projects).
- Many system administrators will say that "it is fun to do."

What makes it even easier is the availability of open source and freeware tools to address some of the pieces of log management for PCI. For example, the following table summarizes a few popular tools that can (and in fact, have been) used in PCI log management projects:

Origin	Tool	License	Purpose	Satisfied PCI Requirement
BalaBit IT	syslog-ng	Open source	General purpose syslog replacement, reliable and secure log transfer	Multiple sections of Requirement 10 and others; enabling infrastructure
Project LASSO	Project LASSO	Open source	Remote Windows event collection	Windows logging centralization; enables analysis of Windows logs covered by Requirement 10
Various	Stunnel, OpenSSH, FreeS/WAN	Open source	Secure data (including log) transfer	Log protection sections in Requirement 10
Various	MySQL, PostgreSQL	Open source and commercial	Data (including log) storage	Log retention section of Requirement 10
Various	swatch, logwatch, logsentry	Open source	Small scripts for log filtering, alerting, and simple monitoring automation	Automated log review in Requirement 10
Risto Vaarandi	SEC	Open source	Log correlation and rule-based analysis	Automated log review in Requirement 10 on a more advanced level
OSSEC team	OSSEC	Open source	Log analysis	Automated log review in Requirement 10 on a more advanced level
OSSIM team	OSSIM	Open source	Log analysis and correlation across logs and other information source	Automated log review in Requirement 10 on a more advanced level

However, if an author's extensive experience with logging is any indication, most if not all projects of this type, no matter how well thought-out and no matter how well funded, will fail. This disturbing outcome occurs due to a combination of these reasons:

- Scalability of the tool when it is being built. It might work great in a lab, but fall completely on its face in a production environment due to data volume, complexities of infrastructure, and so forth.
- Will this tool scale with you or will it require a complete redesign and then rewrite when your environment grows and/or your needs change? Such efforts are usually a big drain on IT teams, since people who might be doing things critical to maintaining a well-oiled "IT machine," all start writing [often bad] code instead.
- Management often likes to point that such approach doesn't pass "the bus test" (Namely, there is no satisfying and credible answer to the question, "What do we do if the smart guy who wrote this wonder of log analysis technology gets run over by a bus?")
- And the final, most terrifying reason: ongoing maintenance of such tool is what deals a mortal blow to many in-house log analysis projects. System vendors change, log formats change, often without notice and without document (provided they did have documents in the first place) thus leading to log analysis system failures with subsequent gaps in PCI-compliance log review or, worse, log collection or retention. We are aware of more than one case where a large corporation abandoned a well-built in-house log analysis tool (with capabilities superior to those of commercial vendors at the time) after spending literally millions of dollars for that reason alone: efforts to update the tool levied a heavy "tax" on team's productivity.

Thus, many people turn to vendors when looking for a PCI logging solution. Commercial log management solutions can aggregate all data from the in-scope entities, whether applications, servers, or network gear. Such solutions enable satisfying the log data collection, monitoring, analysis, data protection, and data retention. (Why do we keep saying "retention" where some people would have used to term "storage?" It is important to note that "retention" usually implies making sure that data is stored for.) Vendors also help with system configuration guidance to enable optimum logging (sometimes for a fee as "professional services"). Advantages of such an approach

are obvious: on day one you get a supported solution as well as a degree of certainty that the vendor will maintain and improve the technology as well as have a roadmap towards addressing other log-related organization needs beyond PCI compliance.

On the negative side of acquiring a PCI logging solution from a vendor sits a landmine of "unmet requirements." It might happen that what was bought and deployed doesn't match what was imagined and needed. Many factors contribute to such a situation: starting from aggressive vendor sales tactics ("overselling"), to insufficient onsite testing, to not thinking about the needs before talking to vendors. Without a doubt, if you "don't know what you need," it is unlikely that you'd buy "exactly what you need."

Fortunately, there are simple things you can do in order to avoid the pitfall of unmet requirements when acquiring a log management solution. Those are:

- Review PCI logging guidance such as this book (as well as the standard itself) in order to clarify the standard's requirements
- Consider how a log management solution would work in your environment
- Define the need by talking to all of the stakeholders in your PCI project and have the above information in mind

Look through the vendor offerings (Web sites, white papers, publications, and so forth) to "case the joint" and to see what is out there.
Congratulations! You are ready to talk to vendors. Here are a few additional questions to ask the vendor:

- Can your tool collect and aggregate 100 percent of all log data from all in-scope log sources on the network?
- Are your logs transported and stored securely to satisfy the CIA of log data?
- Are there packaged reports that suit the needs of your PCI projects stakeholders such as IT, auditors, maybe even Finance or Human Resources? Can you create the additional needed reports to organize collected log data quickly?
- Can you set alerts on anything in the logs in order to satisfy the monitoring requirements?
- Does the tool make it easy to look at log data on a daily basis? Can the tools help you prove that you are by maintaining an audit trail of log review activities? (Indeed, it is common for the auditors to ask for a log that shows that

you review other logs and not for the original logs from information systems! Yes, log analyst activities needs to be logged as well—if this is news to you than welcome to the world of compliance!)

- Can you perform fast, targeted searches for specific data when asked? Remember, PCI is not about dumping logs on tape.
- Can you contextualize log data (say for comparing application, network, and database logs related to an in-scope system) when undertaking forensics and other operational tasks?
- Can you readily prove, based on logs, that security (such as anti-virus and intrusion prevention), change management (such as user account management), and access control policies mandated by the PCI requirements are in use and up-to-date?
- Can you securely share log data with other applications and users that are involved in various compliance initiatives?

Let's take a more detailed look at capabilities of a typical log management solution. The first thing to mention is that such solutions make logs useful for security, IT performance monitoring, system and network troubleshooting, investigations, audit, and compliance such as PCI.

For example, real-time alerting is useful primarily as a threat detection measure. To provide such data protection measures, companies should implement a log management solution that enables administrators to set alerts on all applications, devices, and systems logs. This enables them to provide evidence that the infrastructure has been configured properly and that misconfigured or vulnerable systems are not providing a backdoor for intruders or malicious insiders. Alerts can provide administrators with early warning of misuse and attacks, allowing them to isolate and fix the problem before damage occurs or data is lost, and, of various data access policies and processes not being followed.

Securing the CIA of log data is explicitly mentioned in the PCI requirements above, thus it is crucial to any implementation of a log management tool. This not only serves to reduce the risk of this vital information leaking by means of logs (confidentiality), prevents it from being altered or lost thereby reducing its relevance, immutability, and forensic quality (integrity), but also makes sure that log data is there when you need it (availability). It is hardly possible to say which is the most important and thus the CIA triad lives on.

A need to be able to use logs to address all PCI requirements brings us to access management and change management. While two different areas with little overlap, access and change management are both critical to meeting PCI compliance requirements as well as other regulations and IT governance frameworks, such as ITIL, COBIT, or various International Organization for Standardization (ISO) guidance documents. Strong access and change control measures ensure that only authorized users can access or take action on critical data. The PCI standard mandates that companies maintain a complete record of access (both failed and successful), activity, and configuration changes for applications, servers, and network devices. Logs are that record. Thus, such log data allows IT to set up alerts to unusual or suspicious network behavior and provide information to auditors with complete and accurate validation of security policy enforcement and segregation of duties.

Further, a log management solution allows administrators to monitor who has permission to access or make changes to devices and applications in the network. It also enables administrators to create a complete audit trail across devices, and protect network resources from unauthorized access or modifications. An effective log management tool will support centralized, automated storage of collected data for faster, more reliable data retrieval during an audit or while investigating suspicious behavior.

You probably remember that PCI compliance necessitates ongoing monitoring of network activity (see Requirement 11 and others) to validate that processes and policies for security, change and access management, and user validation are in place and up-to-date.

Logging and monitoring allow for fast problem isolation and thorough analysis when something goes (reactive analysis) or is about to go wrong (proactive analysis). Ongoing and automated log monitoring gives administrators greater insight into the a PCI environment at all times, so that unusual user activity, unauthorized access, or even risky insider behavior can be identified—and stopped—immediately.

In light of the above, the components of an effective log management solution are:

- Collection and aggregation of 100 percent of all log data from in-scope enterprise data sources including firewalls, VPN concentrators, Web proxies, IDS systems, e-mail servers, and all of the other systems and applications mentioned and implied in the PCI standard
- Creation of reports that organize the log data quickly and automatically, so that administrators can deliver detailed network activity information and proof of compliance to auditors.

- Setting of alerts based on changes to individual devices, groups of devices, or the network, to minimize network downtime and loss of data due to malicious attacks, security breeches, insider misuse, or performance issues.
- Fast data retrieval from securely stored, unaltered raw log files. Immutable logs are critical in litigation and attestation.
- Integration with existing network management and security solutions to reduce maintenance and administration and leverage existing architecture.
- The ability to contextualize log data (comparing application, network, and database logs) when undertaking forensics and other operational tasks.

On a more detailed level, here are some sample PCI-related reports and alerts for log review and monitoring.

NOTE

Alerts are only useful if there is a process and personnel in place to intake, analyze, and respond to alerts on a timely basis. In other words, if nobody is wearing a pager or looking for e-mail alerts, they are next to useless.

Alerts – Used For Real-time Monitoring of In-scope Servers

- New account created
- New privileges added to a user account
- Firewall rules change
- Multiple failed logins
- Critical system restarted
- Anti-virus protection failed to load
- Malware detected
- Logs created or log subsystem started
- Log collection failed from an in-scope system

Reports– Used for Daily Review of Pre-analyzed Data

- Risky firewall traffic
- All traffic other than allowed by PCI
- Software update activities
- User account changes on servers (e.g. additions, deletions, modifications)
- Login activity on an in-scope servers
- User group membership changes
- Password changes on in-scope servers and network devices
- All administrator/root activities on in-scope servers
- Log review activities on a log management solution

By now the reader should be convinced that it is impossible to comply with PCI requirements without log data management processes and technologies in place. Complete log data is needed to prove that security, change management, access control, and other required processes and policies are in use, up-to-date, and are being adhered to. In addition, when managed well, log data can protect companies when compliance-related legal issues arise (e.g., when processes and procedures are in question or when an e-discovery process is initiated as part of an ongoing investigation. Not only does log data enable compliance, but it allows companies to prove that they are implementing and continuously monitoring the processes outlined by the requirements.

Case Studies

PCI at a Retail Chain

This case study covers deployment of a log management solution to satisfy PCI requirements at a large retail chain in the Midwest. The Unnamed Retailer, Inc. decided to deploy a commercial log management solution when their PCI auditor strongly suggested that they need to look into it. Given that they have a "unique" combination of a large set of in-scope systems (some running esoteric operating systems and custom applications) and extreme shortage of skilled IT personnel, they chose to buy a commercial solution without seriously considering an in-house development. So, they progressed from not doing anything with their logs directly to running an advanced log management system.

The project took a few months following a phased approached. They decided to implement it from the outside in, based on their risk assessment. They started from their DMZ firewalls and then progressed with feeding the following logs into a log management system, while simultaneously defining alerts and running reports the from vendor's PCI compliance package.

Their project proceeded as follows:

1. All Internet DMZ firewalls
2. Select internal firewalls that control access to payment processing systems
3. DMZ front-end processing servers – operating system only
4. Other payment processing servers – operating system only
5. Databases that are involved in payment processing
6. Actual payment processing applications from all involved servers

A few things need to be said about the above approach. One common piece of technology conspicuously missing from the list is network intrusion detection. The answer is that the organization chose not to implement it due to resource shortage (even though modern NIDses have improved, they still require people to provide care and feeding). The sequence is based on both their risk assessment and the complexity of log collection. The former led them to focus on the outside threat first, while the latter delayed some of the log

Continued

collection efforts: it is much easier to forward Cisco PIX firewall logs to an analysis server, but a database logging configuration, collection and analysis present a significant challenge (due to multiple factors from affecting performance to grabbing logs from a database itself in a secure and reliable manner)

Overall, the project is a successful implementation of PCI logging requirements by using a commercial logging solution. The organization did pass the PCI audit with flying colors and was commended on their comprehensive approach to logging. In addition, the security team built a case that their PCI logging implementation actually addresses a few other compliance mandates (such as US Sarbanes-Oxley act) since PCI DSS goes into a higher level details while covering essentially the same areas of IT governance. At the same time, a log management tools also bolstered their operational capabilities and overall IT efficiency

CI at an E-commerce Site

This case study is based on a major e-commerce implementation of an off-the-shelf log management technology in combination with in-house developed tools to address a unique need alongside PCI compliance. Upon encountering PCI compliance requirements, Buy.Web, Inc developed its own set of scripts to go through order Web server and payment application server logs to identify hacking and fraud attempts. Such scripts were very useful, but proved to be onerous to operate, update, maintain, and troubleshoot. Additionally, a few key IT staffers who helped develop the solution departed to join a consulting company.

Thus, IT management decided to pick a commercial log management application, which will have to work together or integrate with their previous scripts (that still delivered unique value to the organization); they would use a vendor's collection and analysis log management infrastructure, but retain an ability to look for fraud using their own methods.

Their log management project proceeded as follows:

1. Web server logs from DMZ Web servers
2. Operating system logs from the same Web servers
3. Custom payment processing application logs
4. Network logs from the DMZ (firewall, router)

Continued

The project approach was driven by the pre-existing log analysis solution. While the vendor solution was being deployed, they were adapting their scripts to run based on the log management vendor's API, that provided access to pre-analyzed as well as raw log data and allowed the organization to retain a large part of the effort spent on developing the scripts, while at the same time take advantage of the vendor's advanced log management technology as well as regular updater and support.

Overall, this project was a successful illustration of a combined approach of using a homegrown and commercial solution and thus achieving combined benefits (at less than double the cost)

Summary

In conclusion, the authors would like to stress a few points that we covered as well as leave our readers with a few thoughts about how PCI logging fits into the bigger picture of IT governance and risk management. Additionally, we will present a few common mistakes noted in PCI-driven logging implementations.

- Logging in the PCI DSS is not confined to Requirement 10. As we discussed above, all of the requirements imply having a solid log management policy, program, and tools.
- Logging in PCI is not only about log collection retention; Requirement 10.6 directly states that you need to review, not just accumulate logs.
- Log review in PCI does not mean that you have to read the logs yourself; using automated log management tools is not only allowed, but suggested.
- A careful review of what is in-scope must be performed. Otherwise, one creates a possible huge issue for the organization with having what is thought of as a "solid PCI program," but then suffering a data breach and getting fined due to missing a wireless POS system or some other commonly overlooked but clearly in-scope systems. (Well, at least it *became* clear after your organization is fined.)
- Your logging tools purchased and deployed for PCI compliance are almost certainly useful for other things ranging from other compliance mandates (see the above example of PCI and Sarbanes-Oxley) as well as operational, security, investigative, incident response, and other uses.

Solutions Fast Track

- Logging in PCI Requirement 10
- Logging in PCI beyond Requirement 10
- Tools for implementing logging and auditing in PCI
- Reports and alerts for PCI

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to **www.syngress.com/solutions** and click on the **"Ask the Author"** form.

Q: Is all logging in PCI focused on Requirement 10?

A: No, logging is actually present in all 12 requirements of the PCI.

Q: Do I have to manually read all the logs daily to satisfy PCI Requirement 10?

A: No, automated log analysis and review is acceptable and, in fact, recommended.

Q: What are some of the sample reports that users can get from log data to satisfy the PCI requirements?

A: Examples are "User Account Changes," "Account Deleted," "Risky Protocols Use," and others mentioned in the chapter.

Chapter 7

Strong Access Control

Solutions in this Chapter:

- Principles of Access Control
- Authentication and Authorization
- PCI and Access Control
- Configuring Systems to Enforce PCI Compliance
- Physical Security

- ☑ Summary
- ☑ Solutions Fast Track
- ☑ Frequently Asked Questions

Introduction

Access controls are fundamental to good security in almost any situation. We put locks on our cars and homes to protect access to them. We put passwords on computer accounts to protect them. In this chapter, we'll describe some basic security principles that should be understood anytime access control systems are being put into place. By understanding these basic principles, it will be much easier to make individual decisions on implementing access control. After we have a general understanding of access control, we move to the Payment Card Industry's (PCIs) access control requirements. We discuss procedures that should be in place and how systems should be configured to help enforce PCI compliance. After we've shown how to lock down access control on your systems, we move to physically secure systems and media that contain sensitive information.

NOTE

Many times the easiest way to protect data is not to store it at all. It's a good idea to review the data you're keeping and verify that you really need to keep it.

Principles of Access Control

To understand the goals of access controls it's important to understand the three pillars of security: *integrity*, *confidentiality*, and *availability*. As you implement access control in your organization you should always consider these three principles.

Integrity

The principle of integrity means that data has not been altered or destroyed in an unauthorized manner. You must put measures in place to ensure that data cannot be altered while it's being stored or while it's in transit. For PCI compliance, we want to make sure several types of files are protected against modification. This includes files that contain cardholder data, but also includes system files, logs, and other critical files.

Confidentiality

The principle of confidentiality means that we are guarding data from unauthorized eyes. While integrity is primarily concerned with writing (modifying and deleting), confidentiality's primary concern is reading. For PCI compliance, we want to ensure that unauthorized users cannot access cardholder data, particularly not the account number and related information, but again there are many other types of information we need to block from unauthorized eyes. Employee's passwords are not account data, but they are a key to get to it and must be protected.

Availability

The principle of availability means that the data will be accessible to those who need it when they need it. While the first two pillars are concerned with locking down access, this one is concerned with allowing enough access that those who need the data can get to it. For PCI compliance, this means that those employees that need access to cardholder data and other critical information are given it so they can do their jobs.

How Much Access Should a User Should Have

Let's put the principles of integrity, confidentiality and availability into practice. Remember, we want to balance integrity and confidentiality (which both restrict access) with availability (which allows access). To do this we use the principle of least privilege. This means that we want to give an individual enough access so they can do their work, but no more.

An important related term is "need-to-know." This term is used in government to help define what access an individual should be given. Let's say I'm an FBI agent and I have Top Secret clearance. I gained this clearance by proving I was trustworthy through background checks and several years of service. Say one day I'm bored of my work and decide to look at what other Top Secret cases the FBI is investigating. Because of need-to-know, I can't simply start browsing through files that aren't related to cases I'm working on, even though I have Top Secret clearance. If I can't convince my superiors that I need access to information, I will not be given that access. The same rules should apply in your organization. Just because someone works in accounting doesn't necessarily mean they need access to all of your organization's financial information. For example, an employee whose job is to buy inven-

tory to sell likely does not need access to customer's cardholder data, and should therefore be denied access to it.

It's important for you to determine exactly what access a user needs. You need to make sure they're allowed access to those things they need and locked out of everything else. The first thing you need to do is determine what access the user needs to do their job. You should get management involved in this process; management should sign off on a form that approves the specific access a user will be given.

As you are looking at what access a user needs to do their job, make a note of any information they will need access to read but don't need access to write to. For example, an employee may need access to cardholder information to be able to process it, but would never need to change it. In this case, we would set permissions that would protect the integrity of the information. You should also determine if certain data can be retrieved via other employees when needed. For example, an employee may need access to certain financial data only once a quarter. An employee in accounting may work with this data every day and could provide a quarterly report to the employee that needs the data. On the other hand, it wouldn't make sense to have an employee running to another employee every 10 minutes to get information they need to do their job.

Authentication and Authorization

There are three important steps that should happen when an individual is given access to data. These are *authentication*, *authorization*, and *audit*. Authentication is used to determine who the individual is. Once we know whom we're dealing with authorization determines what rights this individual has to access the data. The last step is to audit what the user is doing. This simply means to log what access was approved or disapproved so it can be reviewed later.

Authentication

There are many ways to authenticate a person; in fact we do it many ways on a regular basis. Showing our driver's license to a police officer authenticates us to him. When a police officer shows us his badge we can authenticate him as a police officer. The most common way to authenticate is using a username and password combination. It is assumed if we know both of these pieces of information then we are who we say we are. While none of these forms of authentication are perfect (I could have a fake license, the police officer could have a fake badge, and I could have a stolen

username and password), most of the time they are good enough for what they are being used for.

There are three general ways (often called "factors") to authenticate a person. These are something you know, something you have, and something you are. An example of something you know is a password. This is something you recall from memory that (hopefully) only you would know. Something you have would be something you carry around with you that would help identify you. Some examples of this include a drivers license or some kind of a token such as a SecureID that would be needed to authenticate to the system. Something you are would be a feature you have that distinguishes you from everyone else in the world. Biometrics are often used to identify you by something you are. A fingerprint or hand reader can be used to determine who you are by scanning your hand. Other examples include voice recognition systems, facial recognition systems, and so forth.

Multi-factor Authentication

No form of authentication is full proof. For example, there have been some cases where a biometric fingerprint scanner has been bypassed using a fingerprint from an authorized user. One problem with biometric authentication is if someone figures out a way to impersonate you, you can't change who you are. You can't easily replace your finger if your fingerprint is compromised. Passwords can be guessed and tokens can be stolen.

By using multi-factor authentication, at least two forms of authentication are required before a person is properly authenticated. For example, you would require that a user authenticates themselves using something they know (by typing a password) and something they are (by placing their hand on a biometric scanner). The more factors that are required to identify a person, generally makes it harder to impersonate them. PCI compliance requires that anytime a sensitive system is authorized remotely, at least two factors must be used to authenticate a user before they are given access to the system. To do this authentication, secure remote systems such as Remote Authentication and Dial-in Service (RADIUS) or Terminal Access Controller Access Control System (TACACS) should use at least two factors for authentication.

Passwords

Passwords are interesting beasts. Although they're one of the oldest ways to authenticate to computers, how they should be used is still debated today. Some security

professionals feel strongly that complex passwords are important, while others feel that length is more important. Others say passwords should no longer be used but instead we should be using passphrases (which is basically using a phrase for a password). There are some great arguments for each of these systems, and you should select the ones that work best for your company.

Many security professionals will tell you that a good password should have random uppercase and lowercase letters, numbers, and symbols. While this does make for a good secure password, it also makes it hard to remember. Many times if a user cannot remember the password, they will end up writing it down on a Post-it note and placing it somewhere near the computer such as under the keyboard, in a drawer, or by sticking the Post-it note to the computer screen. This is like having the best lock on a door then putting the key on a nail in the middle of the door.

Other security professionals will argue that longer passwords are better than passwords that use a random complex string of characters. Mathematically, longer passwords make sense because the number of possible passwords increases exponentially as the length of the password increases. Because of this, some will argue that there should be no rules that require certain characters in a password, policies should only require long passwords. While advocates of this make good arguments, this system is not without problems. If an attacker can make some correct assumptions about what types of passwords a user will use, they can make them much easier to crack. For example, if an attacker assumes that the password will be composed of dictionary words that only use lowercase letters, this weakens a password's strength drastically.

Tools & Traps…

The Math of Password Complexity

One measure of password strength is the total possible combinations using your particular character set and length. Generally, the more possible combinations there are, the harder passwords are to crack. For example, using PCI requirements you have 26 lowercase letters, 26 uppercase letters, and 10 numbers. This is a total of 62 total characters.

PCI requires that passwords are at least 7 characters long, so for a 7-character password there would be 62^7 = 3,521,614,606,208 possibilities. Note that the number of possibilities increases exponentially with the length. So, if

Continued

your company required 8-character passwords, then that would be 62^8 = 218,340,105,584,896 possibilities. On the other hand, if you left the length requirement at 7 characters and instead required that users also use symbols in their passwords, then that would add 32 characters to the equation. Now you have 94^7 = 64,847,759,419,264, which is over three times less than if we had instead required the password to be longer.

A passphrase is basically a phrase used in lieu of a password. For example, the phrase "I went to the store at 9:52 and bought bread for $4.29" could be used as a password to log into an account. Advocates of this argue that they are much easier to remember and type (since it's generally easier for people to type words than individual letters) and can have complex characters in them. Generally, passphrases work very well if the phrase is chosen well. For example, the passphrase "thank you" is far less secure than the password above, because of how short it is and the limited number of characters it uses.

PCI Compliant Passwords

PCI requires that passwords are at least 7 characters long and contain numbers and uppercase and lowercase letters. These are minimum requirements and you can strengthen them for your company's needs. For example, although PCI requires that passwords are at least 7 characters long, does not mean your company policy can't require that they're longer. If you wanted to you could also require that passwords contain symbols. Depending on what the password is used for, making the policy stricter than what PCI requirements ask may be complicating things.

Educating Users

While PCI's password requirements are not incredibly strict, they may be much stricter than what your company was using before becoming compliant. If your company is going from a very lax password policy to a stricter one, you will likely meet resistance from employees. Of all the changes you may have to make, this is one that affects employee's day-to-day work. Some employees will have a hard time seeing the benefits from using strict password policies. Some may even grumble that this is just another way the Information Technology (IT) department is making their life harder.

Because of this, it's generally a good idea to meet with employees to explain the policy to them and answer any questions they may have. This is a great opportunity to educate them on what makes a good password and why they are important. It's a good idea to get management involved in this meeting. Many times, if employees see

that management is involved, they take the policy more seriously. You may want to get someone from management to briefly introduce that the company will be implementing a new password policy to help the company become more secure.

One of the things you will want to cover in this meeting is the password complexity requirements that will be enforced. Many times, users get frustrated when it's time for them to change their password, because they don't understand why any of their new passwords are not being accepted. Give them examples of passwords that conform to the policy and ones that don't, and help them see why they don't.

You may also want to go over some tricks to help them choose good secure passwords that will be easy to remember. For example, some security experts advocate writing out a sentence and using the first letter from each word. The sentence should also include numbers. For example, the sentence "I went to Quick SuperMarket today at 9:52 and bought bread for $4.29" would be "IwtQSta9abbf$4". Users could also use a passphrase as long as it has uppercase and lowercase letters and numbers, and that would comply with PCI requirements. There are many other ideas on how to select good secure passwords. A great reference is Mark Burnett's book, "Perfect Passwords." Much of the book is dedicated to helping users select passwords that are unique and easy to remember.

Tools & Traps…

Passwords for Chocolate

Some of the most interesting research in recent years on how well users protect passwords, has been done by the organizers of the Infosecurity Europe. In 2002, they surveyed 150 workers on the way to work, and found that 2 out of 3 were willing to give up their password when asked what their password was as part of a survey (www.managinginformation.com/news/content_show_full.php?id=469). In 2003, the survey participants were offered a cheap pen in exchange for their passwords; 90 percent of the 152 people surveyed gave up their passwords, some after a little coaxing by the person conducting the survey (www.theregister.co.uk/2003/04/18/office_workers_give_away_passwords/). In 2004, they moved from pens to chocolate bars and found that 71 percent of those asked were willing to give up their passwords for the candy (www.enn.ie/frontpage/news-9408519.html). The organizers then decided to wait three years until 2007, to see if the situation had improved. In the 2007

Continued

survey, they also included some of the IT professionals attending the InfoSecurity Europe conference. They found that 65 percent of the 300 people they surveyed were willing to give up their password in exchange for a chocolate bar (www.theregister.co.uk/2007/04/17/chocolate_password_survey/).

Some argue that these surveys don't do anything to verify that the person surveyed wasn't lying about their password, so the numbers are inaccurate. While these numbers may be somewhat inflated, they still give an interesting glimpse into how social engineering and lack of education can be a dangerous combination when mixed with passwords. Users should be educated to never give out their passwords under any circumstances to anyone, including the IT staff. In the 2007 survey, the users were asked if they knew any of their colleague's passwords and 29 percent responded that they did and 39 percent said they would give their password to their IT staff if asked for it. Yikes! Looks like we have a lot of educating yet to do.

This would also be a good time to help them understand how often password changes will be required, and that they will not be allowed to reuse old passwords. You should also review company policies about disclosing passwords. Passwords should never be disclosed to anybody for any reason. Employees should understand the process that's in place to reset their password if they forget it. You should always ask users if they have any questions when rolling out a new policy.

Authorization

After a person has been authenticated, authorization will determine what they can do. This is normally done through some type of access control. Access control systems use subjects and objects to determine access. Subjects are entities that perform actions such as a user or program that does something with a file or other computer resource. Objects are the entity these actions are to be performed against, including a file being accessed or modified.

Most current operating systems use discretionary access control. This means that each object has an owner and that owner decides what access will be given to subjects. In Windows, for example, if I'm the owner of a file, then I can configure who has rights to read and modify my file. This is done using an access control list (ACL), which lists what access each subject is allowed for an object.

Some operating systems are starting to support mandatory access control. For example, Windows Vista has Windows Integrity Control (WIC), which provides mandatory access control that supersedes the discretionary access control set for the file or folder. Previously, this was only found on systems that processed highly sensi-

tive data such as classified files for the government, but it's starting to find its way into mainstream systems. With mandatory access control subjects, objects have labels that specify a level of trust. A subject must have an appropriate label to be able to gain access to an object. An example would be that a subject would have to have top-secret clearance to be able to access top secret objects. Linux distributions are starting to ship with different forms of mandatory access control. For example, Security Enhanced Linux (SE Linux), which was developed by the National Security Agency, is shipped with some distributions of Linux.

When configuring access controls, a good rule of thumb is to first deny all access to objects, then explicitly allow access only to objects that the user needs (PCI Requirement 7.1 mandates you do it this way). This method is called "white listing." In contrast, "blacklisting" is when a subject is given access to all objects by default and the rules are set up to block access to certain objects. Blacklisting generally is harder to maintain and can lead to errors, which could then allow a subject access to objects they shouldn't have access to.

PCI and Access Control

Now that we have discussed some of the basics of access control, we'll show you how to put those into practice for your company. We'll begin by discussing processes that should be in place to comply with PCI requirements. These processes will give you some ideas on how to comply with the PCI requirements in this section that normally cannot be met simply by configuring systems. Next, we will discuss settings that should be configured on various systems to meet with compliance. After that, we'll show how to put these settings into practice on various systems.

NOTE

For some systems, settings will not be available to configure them to comply with some of the requirements we discuss in the "Configuring Systems to Enforce PCI Compliance" section. In that case, you will need to create policies and processes to mandate that they are followed. For example, Cisco systems generally rely on the users to enforce password complexity and history.

Processes for PCI Compliance

To comply with PCI requirements, certain account processes must be in place (e.g., processes for changing, adding, and deleting users must be controlled). These processes should include things such as getting a signed form from the user's manager before creating an account for them, or making any changes to their account. This signed form should be kept on file so it can be used for later review of a users access privileges. If the form is not given to you from the manager, steps should be taken to verify that the request is legitimate.

Any changes to user accounts should be logged and the logs should be periodically reviewed by someone other than the system administrators who makes changes to access controls. This will help protect against a malicious administrator in your organization. When a manager requests new access rights for a user, it's normally a good idea to verify that none of their rights should be revoked. One common problem at many organizations is employees who gain more and more access over time as they change positions, and none of their old access is revoked even though they don't need it anymore.

It is important that a process is in place to properly identify users so you can protect against social engineering. Social engineering is the practice of fooling someone into doing something for you they shouldn't, or giving you information you shouldn't have. Many times it's far easier to get access to confidential data this way than by cracking a password or bypassing a firewall. Policies should be in place that will protect against this as best as possible.

A process must also be in place to securely reset a user's password when it's forgotten. Depending on the size of your organization, the administrator may know each employee and be able to identify them. If you work for a large organization, you may need to have the employee show identification to verify their identity. If a request for a password change is made via telephone, e-mail, or other non-face-to-face method, a policy should be in place to properly identify them.

There are many ways to identify an employee in a non-face-to-face way. One of the most secure ways to identify an employee is to approach them face-to-face and verify they made the request (after asking to see some identification). Many times, depending on the size of your organization, it's unrealistic to hike all around the building identifying employees. Another option is to contact the employee's supervisor or manager to verify that they made that request. Depending on your organization, it may be appropriate to put a more secure system in place to identify

employees over the phone. For example, each employee could be given a secure token such as a SecureID and a pin they give to the IT department to identify themselves. Alternatively, an e-mail that is securely digitally signed could be sent to verify that the employee made the request. Caller ID is generally not a good way to identify users, since it can sometimes be spoofed.

PCI also requires that first-time passwords for accounts are unique. This same process should be followed when resetting passwords (you shouldn't reset all passwords to the same value). It's important to get first time passwords to users in a secure way. Some good ways to do this include sending the password in an encrypted e-mail or other secure channel. If no other secure channel is available, you could also send the password to the user using inter-company mail in a secure envelope (one that you can't easily see through).

Tools & Traps…

Random Password for Users

PCI requires that first time passwords are unique. There are many possible ways to do this. A quick Google search for password generators returns many sites that host password generators. These may work well for you. However, if you're ultra paranoid then you may want to use one installed on your own computer.

Here is a short Ruby script to help you create good first time passwords. Notice that certain letters and numbers will never be used in passwords this program creates. For example 1, l, and I are not included because they can often be mistaken for each other. Also 0 and O have been removed. To run this script you must have Ruby installed (it runs on many operating systems including Windows and Linux) and have the Crypt::ISAAC module, which is a more secure random number generator than the one included with Ruby. This can be found at http://rubyforge.org/projects/crypt-isaac/.

```
#!/usr/bin/env ruby

require "crypt/ISAAC"

rng = Crypt::ISAAC.new
```

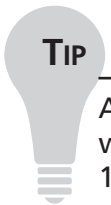
Continued

```
schars = "24356789abcdefghijkmnopqrstuvwxyzABCDEFGHJKLMNPQRSTUVWXYZ"

for i in 1..10
   password = (1..10).collect { |i| schars[rng.rand(schars.length), 1]}
   puts password.join
end
```

A process must be in place to revoke access for terminated employees. Revoking access for terminated employees is both a physical and computer security issue; therefore, you want to coordinate your efforts with physical security people as well. The IT department should be notified so they can revoke the employee's computer access. At the same time, somebody should be with the employee who should then be allowed to gather their personal items and then be escorted out of the building. The employee should not be allowed to continue working on computer systems or do anything where they could compromise systems. While physically escorting a user out of the building may seem like overkill for many terminated users, this is a good process to follow for all users. In this case, it's much better to be safe than sorry. Many times when an employee has just been terminated they are upset and may do things that are out of character. It's also important that the employees name badge is surrendered when they're terminated.

PCI also requires that vendor accounts are only active while they're in use. A good reason to do this is because it helps to limit the ways an attacker can get into your systems. This is called "lowering your attack surface," because it limits the methods an attacker can use. Another good reason to do this is that it follows the principle of least privilege (the vendor doesn't need access so don't give it to them).



TIP

A great way to make sure accounts are disabled is to set an expiration period when the account is activated. By setting a predefined, finite period (such as 10 days, 30 days, or another reasonable fixed amount of time) you will be sure the account will be appropriately disabled.

Earlier in this chapter we talked about password policies and educating users about these policies. It's important that this happens on a regular basis. There are

many ways to educate users, for example, having short classes where you teach or review the policies, or putting up posters to remind users about password policies. After users have been educated on password policies, they should be required to sign off to indicate they understand the policies. This is important to prove compliance and can be used in the future if you need to take disciplinary action against an employee who doesn't follow password policies.

Configuring Systems to Enforce PCI Compliance

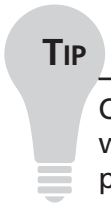
PCI requires that all users be identified using a unique login. This ensures that if an account is used to perform malicious activity, then it can be traced to a specific user. Because of this, group accounts or default logins for users should never be used. Systems must also be configured to use at least one factor of authentication when logging into a machine locally, and two factors when logging in remotely. Acceptable means of single-factor authentication that can be used when logging into a machine locally include passwords, tokens, and biometrics. Remote login should use technologies such as remote authentication and dial-in service (RADIUS) or TACACS that use a token. Remote access may also use a Virtual Private Network (VPN) that uses individual certificates.

All passwords must be encrypted during transmission and storage to protect them from malicious users. Most operating systems will do this for you by default. Poorly configured Cisco devices can store passwords in plaintext, however. It is also import to verify that applications are storing and transmitting passwords securely. For example, an application to store and process cardholder data should encrypt passwords while they are stored and in transit.

All users must be required to change their password at least every 90 days. This makes it harder for a malicious user to crack passwords. For systems that contain sensitive data or that are likely to be attacked (e.g., Web facing systems), it's not a bad idea to change passwords more often (e.g., every 30 days). PCI also specifies several password complexity requirements. Passwords must be at least 7 characters long. All passwords must also contain upper- and lowercase alphabetic characters as well as numbers.

A process should be in place to remove accounts that have been inactive for more than 90 days. Doing this not only keeps your Active Directory tidy (which generally makes it easier to maintain), it also reduces your attack surface. With less active

accounts there are less potential ways for an attacker to gain access. In Active Directory, when new Group Policy password settings are applied, they are only enforced the next time a user changes their password. Because of this, depending on how long the account has been inactive, it could be using a much weaker password than the rest of the accounts on your system and becomes easy prey for attackers.



TIP

One way to force all users to have passwords that comply with the new password policy in the Group Policy, is to set the maximum password age in the policy to 1 day. This will force all users who log in on that day to create a new password that complies with the new policy.

It is also important that users do not reuse any of their last four passwords. This is often called a "password history." The reason this is important is that some users will change their password when the password change is required, and then automatically change it back. By keeping a history, you can verify that they don't reuse old passwords. The problem that remains is that a user can immediately change their password five times and then go back to their original one. To prevent this, it's important to set an appropriate minimum password age. By doing this, a user has to use their password for a predefined amount of time before they can change it to a new one.

Most operating systems allow you to lock out user accounts after a specified number of failed login attempts. To comply with PCI requirements, accounts must be locked after six or more login attempts. Accounts should be locked out for 30 minutes or until the administrator manually unlocks the account. This makes it much more difficult for an attacker to brute force an account. Instead of being able to try several passwords a second, an attacker can only try six passwords every 30 minutes. Also, if a session is left idle for more than 15 minutes, it must require a password to be entered before it can be used. One example of this is enabling a password-protected screen saver. This is important, because sometimes users forget to log out of computers and walk away. If a malicious user were to notice this, they would then have access to the original user's account.

PCI also requires that all access to databases be authenticated. This means that any access to databases by users (including administrators) or programs must be authenticated. This is important to protect the data and allows for auditing access to the database. The same principles should be followed when setting up policies to protect

data in the database, as protecting files in the operating system such as the principle of least privilege. There should be very few individual login accounts on the database server. Most of your access control for individual users should be built into the programs that access the database, and not by giving each individual user an account on the database. Only database administrators should be allowed to execute queries directly on the database server.

Windows and PCI Compliance

If you work in an organization where Windows is widely deployed, you're probably using Active Directory to authenticate users. One of the great things about Active Directory is that it makes it very easy to roll out many of the requirements for PCI. Using Group Policy Objects (GPOs), you can enable password-protected screen savers and set up password policies all from your domain controller. You may also have standalone Windows computers that aren't part of the domain (e.g. a Web server that's at a hosting company), so we'll show you how to configure these for PCI compliance as well.

Windows File Access Control

Windows ACLs or Discretionary Access Control Lists (DACs) are used to configure and enforce access control. ACLs contain a list of Access Control Entities (ACEs), and each entity defines permissions. To set ACLs in Windows, you must have permission. Since Windows uses discretionary access control, the owner of the file and administrators can configure ACLs for an object. When using Windows access control mechanisms, you basically have three options: you can explicitly allow permission, explicitly deny permission, or implicitly deny permission.

When you implicitly deny permission, this means that you did not explicitly allow or deny access. By default, Windows denies all access to objects that do not have rights set on them. This is a great best practice to follow for all systems, and is particularly good because it helps us comply with PCI Requirement 7.2 without doing anything. Because Windows implicitly denies access, explicitly denying access should only be used in special cases where you are denying permission to a subset of a group. One user you would normally never deny access to is the built-in "Everyone" group, because this will deny access to all users including the Administrator. The correct way to do this would be to add users and groups that should have access to the file and then simply remove the Everyone group from the

allowed users. Since Windows follows an implicit deny for anyone not explicitly given permission, this will likely give you the desired result.

WARNING

Sometimes system administrators are lazy and instead of taking the time to set up proper access control, simply give all users administrative rights. This is bad for many reasons, since this gives all users full reign in your network. Also notice, in reality, Windows no longer follows the default deny policy required by PCI Requirement 7.2, since all users are allowed full access to all files.

When configuring access controls in Windows, there are several tricks that can save you time in initial configuration and later maintenance. For example, whenever possible, you should assign permissions using groups rather than individual users. To do this, you would find users whose job functions require that they have the same set of permissions. Then you would create a group and assign all those users to that group. Now you can set access permissions for the whole group instead of each user individually. This also makes maintenance much easier since you can change permissions for the entire group and remove and add users whenever needed. It's not uncommon to have users who are assigned to more than one group. For example, one user may only need access to unprocessed cardholder information, while another user may need access to unprocessed and processed cardholder information. In this case, both users would be members of a group with access to cardholder information, but only the second user would also be a member of a group with access to processed cardholder data.

Another great time saver is to use inheritance as much as possible. When you set permissions on a file or folder, you can also specify how subfolders will inherit those permissions. This makes it much easier to configure access control on a few folders that are near the root folder, instead of needing to configure each subfolder individually. It also can make administering access control easier if you use security templates. This keeps all security settings in the same location and makes them much easier to manage.

WARNING

To be able to effectively secure data in Windows, you should always use the New Technology File System (NTFS). FAT32 does not cut it, because it does not have the capability to do access control.

Creating a New Group Policy Object

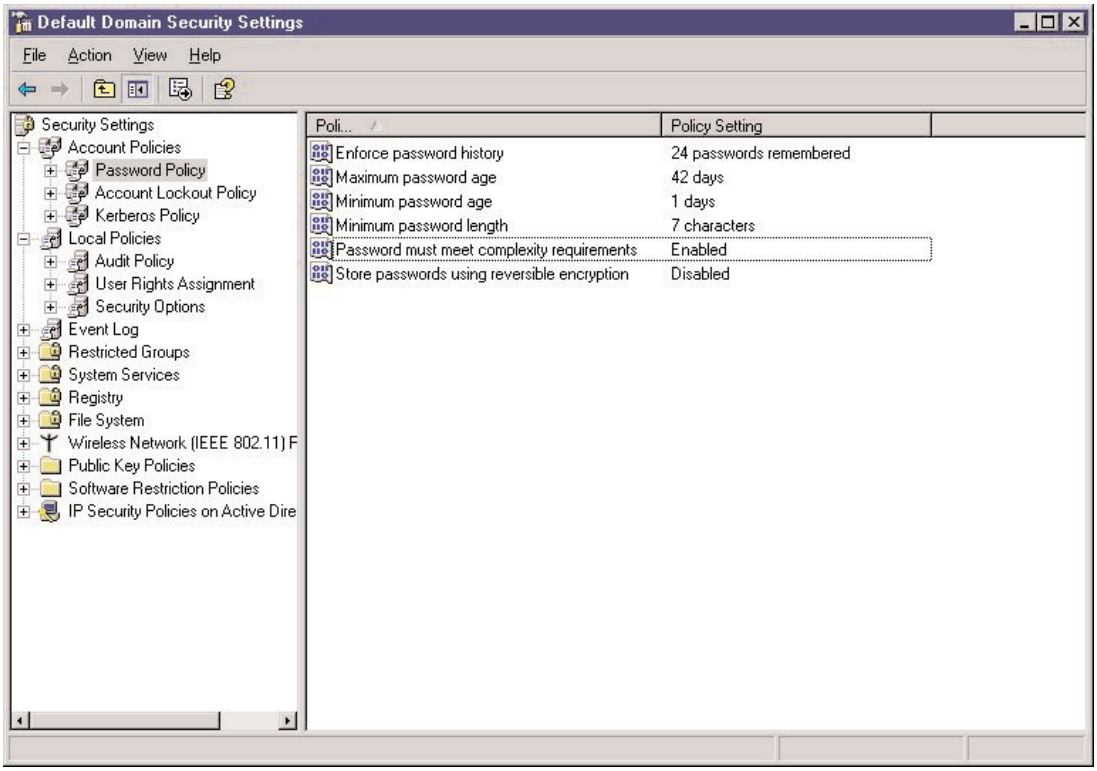
In a Windows Active Directory environment the best way to roll out a password policy to all the computers is to use a GPO. On your Windows 2000 or 2003 server click **Start | All Programs | Administrative Tools**. Inside the Administrative Tools dialog click on **Active Directory Users and Computers**. This will open up a dialog box that will show you your domain as well as several folders for configuring users and computers in your domain.

Right click on your domain and click **Properties**, then click on the **Group Policy** tab. At this point, it is a good idea to create a new policy rather than modifying the default policy. This will make it much easier to revert later if problems occur. To do this, click the **New** button and then give the GPO a name such as **PCI Password Policy**. Next, you will click on your new policy and click the **UP** button. This will move your new GPO in front of the default one so that it will be evaluated before the default GPO. Next left-click on the **PCI Password Policy** and click **No Override**.

Enforcing a PCI Compliant Password Policy in Windows Active Directory

Now that we have our new policy in place, we will configure the password policy on it. Double-click on the **PCI Password Policy** and the "Group Policy Object Editor" should appear. Expand **Windows Settings**, then expand **Security Settings**, then expand **Account Policies**. Next, click on **Password Policies**. In Windows 2003, the default should look like the Figure 7.1

Figure 7.1 Default Windows 2003 Password Policy



- **Enforce Password History** How many passwords should be stored and not allowed to be reused. PCI requires at least four.
- **Maximum Password Age** How often are users required to change their passwords. PCI requires that this happens at least every 90 days.
- **Minimum Password Age** This is used to ensure that users don't change passwords back to the original one, by changing it more times than is in the history and then back to their original. This way they must keep their password for a certain amount of time.
- **Minimum Password Length** This specifies how long the password must be. PCI requires at least 7 characters.
- **Password Must Meet Complexity Requirements** This requires that a password is at least 6 characters long and contains characters from at least three of the following categories:

- Uppercase letters
- Lowercase letters
- Numbers
- Symbol
- Unicode character
- PCI requires that a password has uppercase, lowercase, and numeric characters so this must be enabled to enforce these password complexity requirements.

- **Store Passwords Using Reversible Encryption** This means that passwords will be stored in such a way that they can be retrieved if an application uses protocols that need the user's password. This is not much better than using plaintext passwords, and should therefore be disabled.

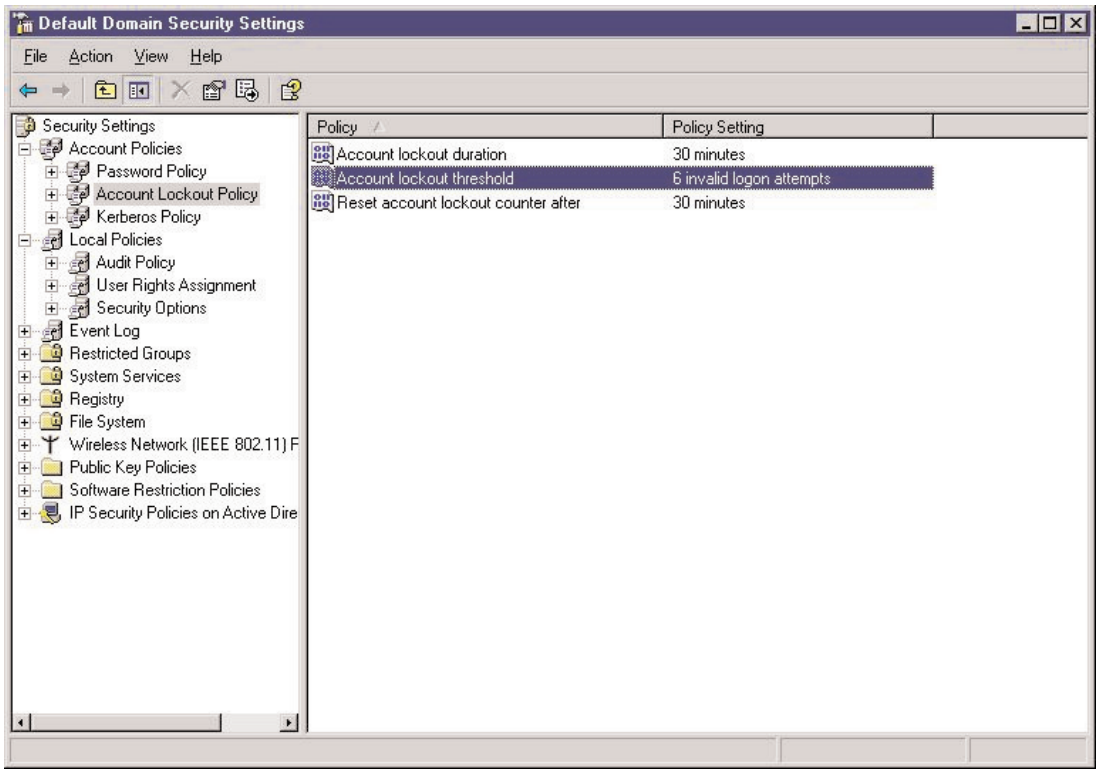
NOTE

Remember that new password requirements will not be enforced until the next password change, so to be PCI compliant today you would have to have all users change their passwords today.

Configuring Account Lockout in Active Directory

While you're configuring the password policy settings, it's a good idea to also configure the account lockout policy. To do this expand **Account Lockout Policy**. Double click on **Account lockout threshold**. In the Account lockout threshold Properties dialog box, change **number of invalid login attempts** to **6**. A dialog box will pop up and ask if it should also change the Account lockout duration and Reset account lockout counter after attributes as well. These should both be changed to **30 minutes** to comply with PCI requirements, which is what the default is in this new dialog. Click **OK.** It should now look like Figure 7.2.

Figure 7.2 PCI Compliant Windows 2003 Account Lockout Policy



Setting Session Timeout and Password-protected Screen Savers in Active Directory

Under **User Configuration** go to **Administrative Templates | Control Panel | Display**. Double-click on **Activate screen saver**, click the radio next to **Enabled** and then click **OK**. This will enable screen savers on all client machines. Now double-click on **Screen saver executable name** and click the radio next to **Enabled** and in the text box type **scrnsave.scr** (see Figure 7.3).

This will enable a blank screen saver on all computers in the domain. Now double-click on **Password protect screen saver**, click the radio next to **Enabled**, then click **OK**. Last but not least, click on **Screen saver timeout** then click on the radio next to **Enabled**. PCI requires that all sessions timeout after 15 minutes which is equivalent to **900** seconds (see Figure 7.4).

Figure 7.3 PCI Compliant Windows 2003 Screen Saver Properties

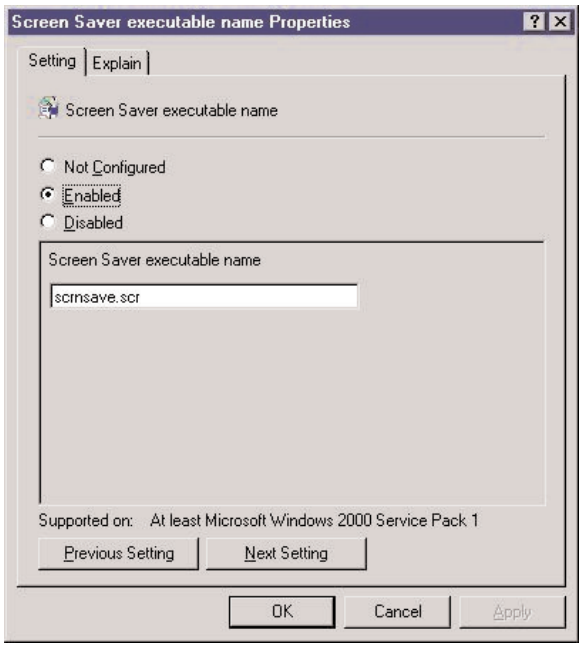
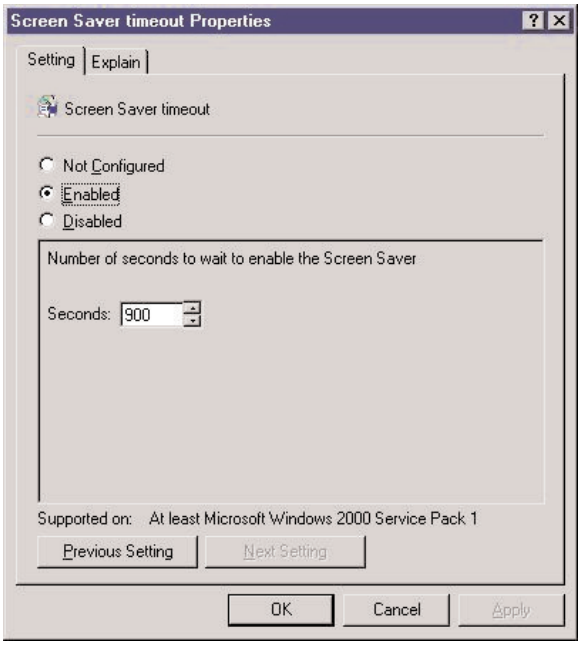
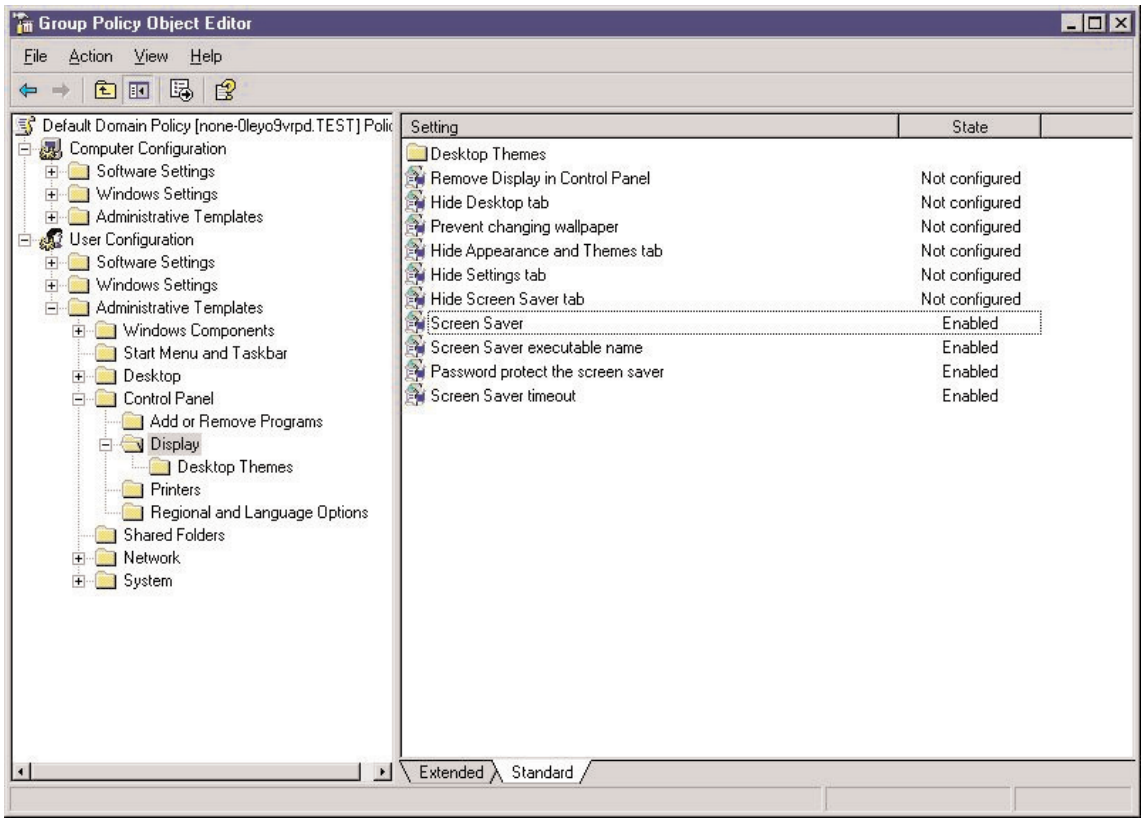


Figure 7.4 PCI Compliant Windows 2003 Screen Saver Timeout Properties



That's all there is to it. Now all of the sessions on your Windows machines in your domain should time out after 15 minutes and require a login to get back in. In the end your screen should look Figure 7.5.

Figure 7.5 Windows 2003 Display Properties

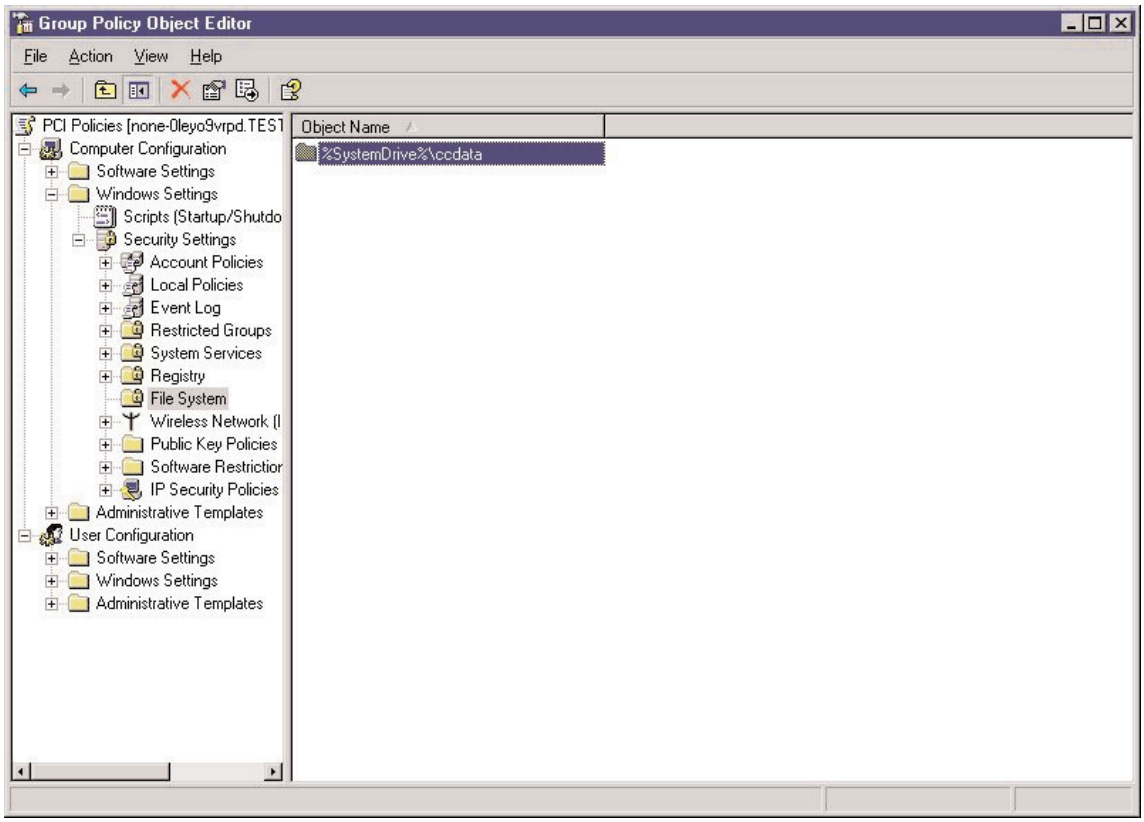


Setting File Permissions Using GPOs

We recommend that you use the GPO to set permissions for the file system. This makes permissions easy to maintain and keeps all of your security settings in one place.

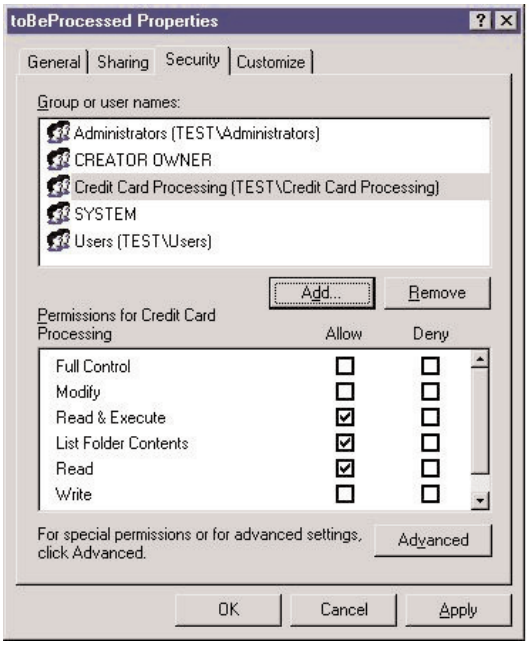
In the GPO that we created in the last section, go to **Windows Settings | Security Settings**. Click on **File System** and you will see a list of any files that have permission set on them in your GPO. To change the settings on a file currently listed, double-click on the file and a **Properties** dialog box will open. You can change inheritance settings in this dialog box to tell Windows how subfolders permissions should be effected (see Figure 7.6).

Figure 7.6 Windows 2003 Access Control



Click on **Edit Security** and a dialog box will open that will allow you to view and modify what kinds of rights user and group accounts have. To add a user or group to the list of Group or user names, click on the **Add** button and the Select Users, Computers, or Groups dialog box will appear. You can then type in the name of a user or group. The Advance button will give you more options to help you find the correct group or user to add. After you click **OK**, the user or group will appear in the previous dialog (see Figure 7.7).

Figure 7.7 Windows Access Control Settings



By clicking on the **Advanced** button you can view and change special permissions settings. You can also modify auditing settings and owner settings using the Auditing and Owner tabs.

Finding Inactive Accounts in Active Directory

One of the PCI requirements is to find all accounts that have been inactive for 90 days or more and remove them. In Active Directory, there are several ways to find inactive accounts. If you are using Windows 2003, you can use the built-in *dsquery* tool. To find all users who have not logged in the last 90 days the syntax is:

```
dsquery user -inactive 13
```

This command uses 13, because this expects the query in weeks, which equals 91 days. For Windows 2000, there is a tool called *OldCmp* available at www.joeware.net. This tool works with both Windows 2000 and 20003, and has features to not only find inactive accounts, but to automatically delete them as well. It also makes easy-to-read reports in Hypertext Markup Language (HTML). Windows 2000 does not have a method to return the last time a user logged into an account, this was added to 2003. We can, however, tell when a user's password was last changed. Since PCI requires that passwords are changed at least every 90 days if a password has not been

changed in the last 180 days, then it has been inactive for at least 90 days. If you have configured your system to require that users change their passwords more often than 90 days, it would be that amount of time plus 90. *OldCmp* should be executed from the command prompt of the domain controller. The syntax to find inactive accounts using *OldCmp* is as follows:

```
oldcmp -report -users -b dc=mydomain,dc=com -age 180 -sh
```

If you would like to use *OldCmp* against a Windows 2003 to do the same thing, the syntax would be:

```
oldcmp -report -users -b dc=mydomain,dc=com -llts -age 90 -sh
```

After these are run, a browser window will automatically appear with a report in it of what *OldCmp* found. You can then review this list of accounts to verify that there's no good reason for the account to have been inactive (e.g., that person has been on the road for a long time and will return shortly). After you have reviewed, you can use the *–forreal* switch, which will tell *OldCmp* to delete the inactive accounts it reported previously.

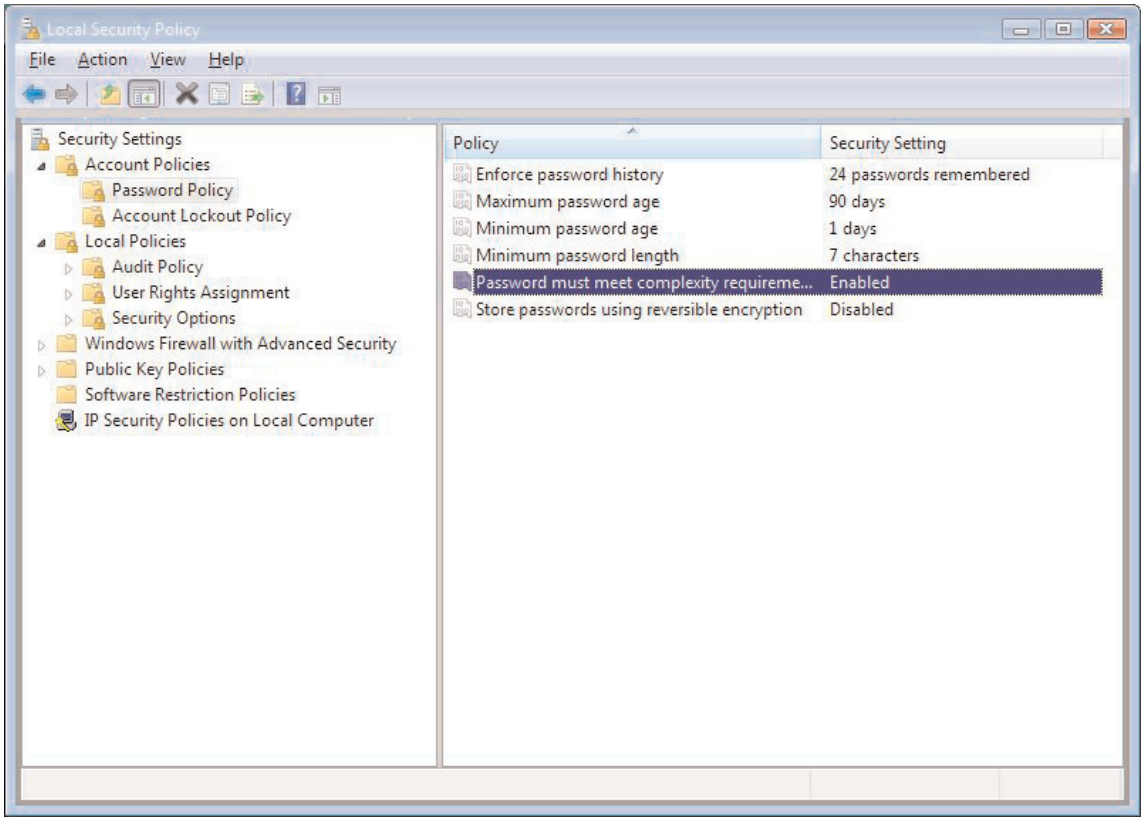
Enforcing Password Requirements in Window on Standalone Computers

To set password policies for a Windows computer (including 2000, XP, 2003, and Vista) that is not connected to the domain, you should use the Local Security Settings dialog box, which is set up basically the same way as the GPO used in the last few sections, except that it will only affect the local computer.

- **Windows XP** Click on **Start | Control Panel**. Inside the Control Panel click on Performance and Maintenance **| Administrative Tools | Local Security Policy**.
- **Windows 2000** Click on **Start | Programs | Administrative Tools**. Inside the Administrative Tools dialog box, click on **Local Security Policy**.
- **Windows 2003** Click on **Start | All Programs | Administrative Tools**. Inside the Administrative Tools dialog box, click on **Local Security Policy**.
- **Windows Vista** Click on **Start | Control Panel**. Inside the Control Panel dialog box click on **System Maintenance | Administrative Tools**. In the Administrative tools dialog box, click on **Local Security Policy**.

You should now have a dialog box open that looks something like Figure 7.8.

Figure 7.8 Windows Vista Default Password Policy



Now expand **Account Polices**, then click on **Password Policy**.)For an explanation of what these settings mean please refer to the earlier section called Enforcing a PCI Compliant Password Policy in Windows Active Directory.) Enforce password history should be changed to at least 4 to meet PCI requirements. The Maximum password age should be set to at most 90 to meet PCI requirements. The password length should be at least 7 characters for PCI requirements, and passwords must meet complexity requirements and should be set to enabled. It's also a good idea to set the Minimum password age to at least 1. Otherwise, when a user is required to change their password, they could change it four times then back to their original password. When this setting is set to 1 or more, the user must keep the same password for at least that many days before they can change it again.

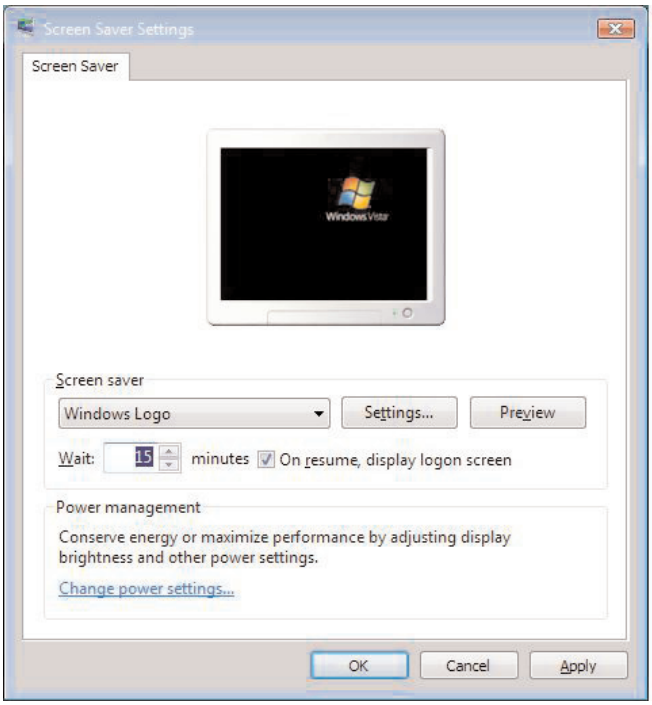
You should also configure the Account Lockout Policy to comply with PCI requirements. To do this expand **Account Lockout Policy**. Double click on **Account lockout threshold**. In the Account lockout threshold Properties dialog box change **number of invalid login attempts** to **6**. A dialog box will pop up and ask if it should also change the Account lockout duration and Reset account lockout counter after attributes as well. These should both be changed to 30 minutes to comply with PCI requirements, which is what the default is in this new dialog. Click **OK.**

Enabling Password Protected Screen Savers on Standalone Windows Computers

Setting screen saver options is much easier to maintain and enforce using Active Directory. If you have computers that are not connected to a domain, these options can be set on each computer individually.

- **Windows 2000, XP and 2003 Server** Click on **Start | Control Panel**. In the Control Panel double-click on **Display**. Inside the display dialog click on the **Screen Saver** tab. The **Wait** option should be set to 15 minutes at the most. Also verify that **On Resume, password protect** is checked**.**
- Windows Vista Click on **Start | Control Panel**. In the Control Panel, click on **Personalization** then on **Screen Saver**. In the Screen Saver dialog box set the Wait time to a maximum of 15 minutes. Also verify that **On Resume, display logon screen** is checked.

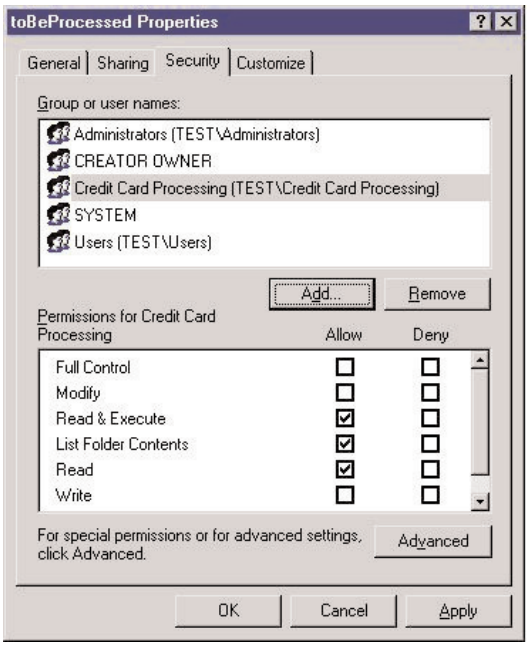
Figure 7.9 Windows Vista Screen Saver Settings



Setting File Permissions on Standalone Windows Computers

In Windows Explorer, navigate to the file or folder you would like to modify permissions on. Right-click on the file or folder then click on **Properties**. In the Properties dialog click on the **Security** tab. To add a user to the list of Group or user names click on the **Add** button and the Select Users, Computers, or Groups dialog box will appear. You can then type in the name of a user or group. The Advance button will give you more options to help you find the correct group or user to add. After you click **OK**, the user or group will appear in the previous dialog box (see Figure 7.10).

Figure 7.10 Windows Access Control Settings Dialog



By clicking on the **Advanced** button, you can view and change special permissions settings. You can also modify Auditing settings and owner settings.

POSIX (UNIX/Linux-like Systems) Access Control

UNIX-based systems such as Linux used POSIX-style access control lists. This means files have three permission modes: *read* (*r*), *write* (*w*), and *execute* (*x*). These modes came be assigned either using the letters just listed or they also have equivalent numbers. Read is *4*, write is *2*, and execute is *1*. If file permissions are being set using letters, it will be a string of letters or dashes (e.g., a file with read only permission would show *r--*, a file with read, write and execute would show *rwx*, and so forth). When using numbers, they are added to denote permissions. Read permission would simply be a 4, read and write permission would be *6* (4 plus 2). When using POSIX-style access controls, there are three groups or users you set permissions for. The first set is for that specific user who owns the file. The second set is for the group who owns the file. The third is for all other users who do not have any ownership over the file. So, a file that allows the owner to read, write, and execute and everyone else only read access would look like this *–rwxr--r--* or in numeric format it would be *744*.

Linux has great command line tools for changing file permissions and file ownership. While exploring all that these commands can do is beyond the scope of this book, we will discuss some basics here. In Linux, to list file permissions, the *ls* command can be used. The syntax to list the file permission and the group and user who own the file is:

```
ls -lg [filename]
```

To change file permissions in Linux, you usually use the *chmod* command. You can run the *chmod* command using numbers. The following example uses POSIX permission number format to set a file to allow the user who owns it to read, write, and execute the file, and everyone else to read and execute (no write).

```
chmod 755 filename
```

Or you could use letters and specify if you are going to add them or delete them from users (*u*), groups (*g*), others (*o*), or all (*a*). For example, to allow the user who owns the file to read from it and write to it you would do the following:

```
chmod u=rw filename
```

To take away permissions use a – in front of the permissions parameter. To deny read, write, and execute permission to the group that owns the file and to all users other than the one that owns the file, you would do the following:

```
chmod go-rwx filename
```

To change the file ownership use the *chown* command. To change the user and group that owns a file do the following:

```
chown newuser:newgroup filename
```

In POSIX-style systems, there are three additional attributes that affect how files are executed are accessed. These are set user ID (SUID), the set group ID (SGID), and sticky. These settings work differently when they're applied to files or directories. The SUID bit can be configured to tell the file what user it should run under when the file is executed. Many times this is used to allow a non-root user to run a file as the root user. This is used if a user needs to run a file that requires root access and you don't want to give their account root access or the root password. SGID for a file works the same way as SUID, but it specifies what group the file should execute as. The sticky has no effect on individual files. The SUID bit has no effect on directories. If the SGID bit is set on a directory, any new files created in that directory will be owned by the group specified using the SGID instead of the group of the

user who created the file. This is sometimes used in directories where many users will share files. When the sticky bit is set on a directory, only the user owner of the file or root can delete or rename a file (the group owner cannot). This is sometimes used in shared directories where you don't want users other than the owner or root to delete or rename a file.

In Linux, there are also several mandatory access control systems. Most of them are somewhat limited to protecting only a subset of files on the system (normally only critical system files). SE Linux is it an example of this. SE Linux was developed by the National Security Agency (NSA) and has been incorporated into the 2.6 series Linux kernel. SE Linux uses targets to specify what files it will control and how it will control them. Other mandatory access control systems that are currently being used in Linux include Suse's AppArmor, Rule Set Based Access Control (RSBAC).

Linux Enforce Password Complexity Requirements

Most Linux distributions support password complexity enforcement using the PAM module. This is normally set in */etc/pam.d/system-auth*. To comply with PCI requirements, a password must be 7 characters long and contain uppercase, lowercase, and numeric characters. *Pam_cracklib* has parameters to help you meet these requirements. The *minlen* parameter is used to specify the minimum length of a password. The *dcredit* parameter is used to requite digits, the *ucredit* is used to require uppercase letters, and the *lcredit* parameter is used to require lower case letters. The *retry* parameter is used to specify how many attempts a user gets before the password program exits. Let's put all these together:

```
password      required      /lib/security/pam_cracklib.so minlen=7 dcredit=1
ucredit=1 lcredit=1 retry=5
```

Cisco and PCI Requirements

Cisco devices have some important settings that should be used for you to become PCI compliant. All passwords should be encrypted when stored or in transit. Most operating systems will do this and not really give you an easy way to store them unencrypted even if you want to. Cisco devices are an exception, however, so it's important to check this.

CISCO Enforce Session Timeout

To force Cisco devices to automatically timeout if a session is left inactive, use the *exec-timeout* command. The syntax for this command is exec-timeout minutes seconds. For PCI compliance this should be set to:

```
exec-timeout 15 0
```

Encrypt Cisco Passwords

The current best practice from Cisco is to always use "enable secret" and "username secret," instead of enable password. Enable password encrypts the password using a very weak encryption algorithm that has been broken for a long time. The secret command uses Message Digest 5 (MD5) to hash the password. While MD5 has shown some weaknesses lately, this is far better than the alternative and the best Cisco is giving us right now.

Database Access and PCI Requirements

PCI requires that all access to databases be authenticated. You should make sure that all accounts are well protected with good strong passwords. One account that you should take special note of is the administrative account. On some systems, the default password is blank; on others it is a widely known default value. Verify that this password is not blank of an insecure default.

Physical Security

There are three basic types of physical security. The first type is obstacles such as doors, walls, and other barriers, which can help stop or at least delay intruders. The second type is detection mechanisms such as alarms, lighting, guards, and television cameras that help detect attacks. The third type is response, which includes things you would put in place to stop an attack in progress or soon after. It's important to use all of these types of physical security to protect sensitive information. For example, you may put sensitive data behind a locked door and have security cameras monitoring that door recording everybody who goes in and out. You may also have a guard on duty that can quickly respond to stop anyone who's trying to circumvent the lock. Sometimes it's advised to have security measures in plain sight, that way they will deter attackers from trying in the first place.

To comply with PCI requirements, cameras must be in place to monitor secure locations. The tapes should be audited and the data should be correlated with other entries. Tapes should be kept for at least three months, unless laws in your area prohibit storing them for that long. It's important to store these tapes so that if an attack is discovered, they can be reviewed to find as much information as possible. These tapes should be securely stored where they cannot be altered or stolen.

Steps should be taken to limit access to publicly network jacks. If an attacker can enter your environment and connect their computer directly into a network jack, he may be able to gain access to your network without needing to bypass your firewalls and other security measures. Hopefully, the publicly available network jacks in your organization are segmented from your internal network in some way. Even if they are, it's best to keep a close eye on these ports. If these ports are available in conference rooms, a policy should be in place to require that these rooms are locked when they're not in use. Anytime someone from outside the organization is in a room with publicly available network jacks, they should be escorted by someone from your organization.

Network devices such as gateways, handheld devices, routers, and wireless access points should be physically secured as well. If an unauthorized person gains physical access to these, they may be able to change configuration settings on them to allow them to bypass security settings so they can have access to your network. An even simpler attack would be to pull the plug on these devices to cause a Denial-of-Service (DoS) attack.

Visitors

A process should be in place to help distinguish employees from visitors. Visitors should be given some type of physical token, such as a name badge that easily distinguishes them from an employee. It's important that these badges are easily distinguishable from a distance, or they will likely not be noticed. A good way to do this is to have a visitor's badge be a different color and shape than an employee's badge. Visitor's badges should also have something on them that denotes when they expire so that the badge cannot be used later. Whatever type of physical token a visitor is given when they arrive, should be surrendered when a visitor leaves. Enforcing this will make it harder for a visitor to re-enter later. A log of all visitors including times they arrived and left should be kept for at least three months, unless this is prohibited by your local laws. By keeping these laws, you have a record to review at a later date if you need it.

NOTE

While you're reviewing visitor's badges, it may be a good time to look at employee badges. There may be some simple changes you can make to them that will help you physically secure your company. For example, sometimes pictures on employee badges are very small and are hard to see from even a few feet away, and therefore are rarely ever looked at.

Employees should be trained in your policies for visitors. For example, employees should know what a visitor's badge looks like and how to tell if it's expired. Visitors should also be authorized before entering any area where cardholder data is processed or maintained. In most cases, visitors should always be attended from when they enter your organization to when they leave. Employees should know what to do if they see a visitor unattended, especially if they are in a sensitive area, such as areas where cardholder data is processed and stored. A good policy to have is that if an employee reports a suspicious visitor, they will receive some kind of reward. This could include things like a small amount of paid time off or a letter of commendation in their personal file.

Physical Security and Media

In previous sections of this chapter, we've gone to great lengths to secure data on systems, but this is all in vain if an attacker simply walks off with a drive (or the whole system itself). Media backups must be stored in a secure location. It is best if media is stored off-site, such as at a backup site or a commercial backup facility. This way, if your building burns to the ground, then you will still have backups of your data. The backup location should have physical security measures in place and the backups should be stored in a fireproof location. You should visit this location on occasion to verify that your backups are being stored correctly.

Any media that contains cardholder data must by physically secured. Computers, drives, disks, and networking equipment that store cardholder data should be kept in a secure area behind locked doors. It is also a good idea to securely attach computers and other systems (such as networking equipment) to racks or desks so they cannot be easily stolen. It is also important to physically secure telecommunication lines within your organization that carry cardholder data, so they cannot be tampered with.

All paper media that contains cardholder data must also be physically secured. This includes paper receipts, paper reports, and faxes. These should all be stored in locked secured areas. If faxes are being received that contain cardholder data, the fax machine they arrive on should also be kept in a secure location. Any media that contains cardholder data should be marked confidential. This makes it easier to track this media and reminds employees of the importance of keeping this media secure. If cardholder data on media is shipped off-site, it should be sent using a secured courier or one that can be accurately tracked. Before handing media over to anyone from a secured or other courier, ask them for identification to verify they are an employee for the company. FedEx, UPS, and Airborne all give their employees identification badges and you should see these before handing over the packages containing sensitive media.

Management must approve and sign-off on all media that is being moved from secure areas (especially if it is being distributed to individuals). Management should be well trained to know company policies on when media should be allowed to leave secured areas. Media should be strictly controlled and regularly inventoried. This ensures the media has not left that was not recorded. When you are doing an inventory of media, if you discover media containing sensitive data is missing, it should be investigated immediately. During this inventory, you should verify that all media is being properly and securely stored.

Media containing sensitive data should be securely destroyed when it is no longer needed for business or legal reasons. For paper, this could include shredding, incinerating, or pulping. Electronic media should also be securely destroyed. This can be done by degassing, purging, or shredding a hard drive. While media is being stored, before destruction it should be in a securely stored container. For example, a trash bin that stored paper that will be shredded should be locked and kept in a secure location.

NOTE

Many companies outsource secure destruction of media. If possible, choose a company that will do the destruction at your site so you can watch them.

Summary

Access controls are an extremely important part of protecting your data. It is important to understand your systems and the best ways to control access to your data. Once access controls are set, they must be constantly maintained to be effective. As we have talked about in this chapter, it's important to have many layers of security to be effective. Not only is it important to have strict access controls in place on computer systems, it's also important to control physical access as well.

Solutions Fast Track

Principles of Access Control

- ☑ Integrity is used to protect data from being altered
- ☑ Confidentiality is used to protect data from being read
- ☑ Availability is used allow data to be used by those authorized

Authentication and Authorization

- ☑ Authentication is the process of verifying a users identity
- ☑ Authorization is deciding what authenticated users can do

PCI and Access Control

- ☑ Proper procedures must be in place so employees will know how to properly protect data
- ☑ System settings should be used to enforce PCI compliance

Configuring Systems to Enforce PCI Compliance

- ☑ Windows systems should be configured using Active Directory when possible, but can be configured as standalone systems as well
- ☑ Configuring other systems such a Linux and Cisco

Configuring Systems to Enforce PCI Compliance

- ☑ Cameras and locks should be used to protect sensitive data
- ☑ Proper procedures should be in place to securely deal with visitors
- ☑ Media containing sensitive data must by physically secure

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to **www.syngress.com/solutions** and click on the **"Ask the Author"** form.

Q: Are there other settings on Linux servers that can help me enforce PCI compliance?

A: Yes there are. On most Linux distributions, you can enable a password protected screen saver just like we did in Windows (in fact some distributions have it enabled by default). Also, if you're using a Linux-based Lightweight Directory Access Protocol (LDAP) server such as OpenLDAP instead of Active Directory, you can enforce many of the same rules. Most of these settings were not covered in this chapter, because of the variety of distributions and differences in each which made it beyond the scope of this book.

Q: Currently my organization has very little access control in place on computer systems. What's the best way to make the move to stricter controls?

A: Like any configuration change, it's important to test systems thoroughly before rolling it out to the whole company. Of all the settings on computers, access controls can sometimes be the most frustrating, which is why some organizations are so lax in their access controls. A good thing to do is to start with the most sensitive data and make sure access is strictly controlled, and then move on from there. Whenever you make any changes to systems, you should always have a back-out procedure in place just in case things don't work out.

Q: If you were to design a badge for visitor, what would it look like?

A: It would be an obvious bright color like red or orange (unless employee badges are red or orange) that could be seen from a distance. They would say the word Visitor on them in big letters, with an expiration date and time on them. It would also have the visitor's name on it in large letters.

Chapter 8

Vulnerability Management

Solutions in this chapter:

- Vulnerability Management in PCI
- Requirement 5 Walkthrough
- Requirement 6 Walkthrough
- Requirement 11 Walkthrough
- Common PCI Vulnerability Management Mistakes
- Case Studies

- ☑ Summary
- ☑ Solutions Fast Track
- ☑ Frequently Asked Questions

Introduction

Before we dive deep into Payment Card Industry (PCI) requirements related to vulnerability management, and find out what technical and non-technical safeguards are prescribed there, we need to address one underlying and confusing issue of defining some of the terms that the PCI Data Security Standard (DSS) documentation relies upon. These are:

- Vulnerability assessment
- Penetration testing
- Testing of controls, limitations, and restrictions
- Preventing vulnerabilities via secure coding practices

Defining vulnerability assessment is a little tricky, since the term has evolved over the years. For instance, Wikipedia (http://en.wikipedia.org/wiki/Vulnerability_assessment) defines it as "the process of identifying and quantifying vulnerabilities in a system," which is a very broad definition. In the realm of information security, vulnerability assessment is usually understood to be a vulnerability scan of the network with a scanner, implemented as software, dedicated hardware, or a scanning service. Sometimes using the term "network vulnerability assessment" adds more clarity to this. Terms "network vulnerability scanning" or "network vulnerability testing" are usually understood to mean the same.

Penetration testing is usually understood to mean an attempt to break into the network by a dedicated team, which can use the scanning tools mentioned above, and also other non-technical means such as dumpster diving (i.e., looking for confidential information in the trash), social engineering (i.e., attempting to subvert authorized Information Technology (IT) users to give out their access credential and other confidential information). Sometimes, penetration testers might rely on other techniques and methods, such as custom written attack tools.

Testing of controls, mentioned in Section 11.1, does not have a simple definition. Sometimes referred to as a "site assessment," such testing implies either an in-depth assessment of security practices and controls by a team of outside experts, or a self-assessment by a company's own staff. Such control assessment will likely not include attempts to break into the network.

Preventing vulnerabilities, covered in Requirement 6, addresses the vulnerability management by assuring that newly created software does not contain the known

flaws and problems. Requirements 5, 6, and 11 also mandate various protection technologies, such as anti-virus, Web firewalls, intrusion detection and prevention, as well as others.

The core of PCI Requirement 11 covered in this chapter covers all of the above and more. The requirement covers all of the above types of testing as well as some of the practices that help mitigate the impact of problems, such as the use of intrusion prevention tools. Such practices fall into broad domains of vulnerability management and threat management. It is worthwhile to note that while there are common definitions of vulnerability management (covered below), threat management is typically defined ad hoc as "dealing with threats to information assets."

Vulnerability Management in PCI

Before we start our discussion of the role of vulnerability management for PCI compliance, we need to briefly discuss what is covered under vulnerability management in the IT industry. It appears that some industry pundits have proclaimed that vulnerability management is simple: just patch all those pesky software problems and you are done. Others struggle with it, since the scope of platforms and applications to patch and other weaknesses to rectify is out of control in most large organizations with compliance networks and large numbers of different products. However, vulnerability management is not the same as just keeping your systems patched. If you are busy every first Tuesday when Microsoft releases its batch of patches, but not doing anything to eliminate a broad range of enterprise vulnerabilities during the other 29 days in a month, you are not managing your vulnerabilities efficiently if at all.

Clearly, vulnerability management is not only about technology "patching the holes." As everybody in the security industry knows, technology for discovering vulnerabilities is getting better every day. Vulnerability scanners can detect vulnerabilities from the network side with reasonable accuracy, as well as from the host side with even better accuracy. However, many organizations that implemented periodic scanning have discovered that the volumes of data far exceed their expectations and abilities. A quick scan-then-fix approach turns into an endless wheel of pain. Many free and low cost commercial-vulnerability scanners suffer from this more than their higher-priced brethren, thus exacerbating the problem for price-sensitive organizations such as smaller merchants. Using vulnerability scanners efficiently presents other challenges as well as, including having network visibility of the critical systems, perceived or real impact on the network bandwidth, as well as system stability. Overall, it

is becoming more clear that vulnerability management involves more process than technology, and should be based on the overall risk and not simply on the volume of incoming scanner data.

Let's outline some critical stages of the vulnerability management process. Even though Gartner analysts have defined that the vulnerability management process includes the steps below, vulnerability management starts from software creation when vulnerabilities are actually introduced. Thus, investing in secure coding practices (prescribed in Requirement 6) helps make the vulnerability management lifecycle much less painful. The following steps are commonly viewed as composing the vulnerability management process:

1. Policy definition is the first step and includes defining the desired state for device configurations, user identity, and resource access.
2. Baseline your environment to identify vulnerabilities and policy compliance.
3. Prioritize mitigation activities based on external threat information, internal security posture, and asset classification.
4. Shield the environment, prior to eliminating the vulnerability, by using desktop and network security tools.
5. Mitigate the vulnerability and eliminate the root causes.
6. Maintain and continually monitor the environment for deviations from policy and to identify new vulnerabilities." ("Improve IT Security With Vulnerability Management" by Amrit T. Williams and Mark Nicolett, Gartner, May 2005.)

Indeed, the vulnerability management process starts from the policy definition that covers organization's assets, such as systems and applications and their users, as well as partners, customers, and whoever else touches the resources. Such documents and the accompanying detailed security procedures define the scope of the vulnerability management effort as well as postulate a "known good" state of those IT resources. Policy creation should involve business and technology teams, as well as senior management who would be responsible for the overall compliance. PCI DSS requirements directly affect such policy documents, and mandate its creation (see Requirement 12 that states that one needs to "maintain a policy that addresses information security"). For example, marking the assets which are in-scope for PCI compliance is also part of this step.

The data acquisition process comes next. A network vulnerability scanner or an agent-based host scanner is a common choice. Both excellent freeware and commercial solutions are available. In addition, emerging standards for vulnerability information collection, such as OVAL (http://oval.mitre.org), as well as established standards for vulnerability naming, such as CVE (http://cve.mitre.org), can help provide a consistent way to encode vulnerabilities, weaknesses, and organization-specific policy violations across the popular computing platforms. While unlikely, there is a chance that your PCI auditor will ask to see this raw data, not just reports that indicate that you are "doing great." One interesting note on this comes from the author's own experience with vulnerability scanning for compliance purposes: an auditor not only asked to see a list of discovered vulnerabilities (which, understandably, all scanners do), but also a list of vulnerabilities that were checked for and found to be absent (which, unfortunately, not all scanners do). This shows that while "scanning for remediation" only requires a list of vulnerable systems with their vulnerabilities, "scanning for compliance" also calls for having a list of systems found not to be vulnerable.

The next phase, prioritization, is a key phase in the entire process. It is highly likely that even with a well-defined specific policy and a quality scanner, the amount of data on various vulnerabilities from a large organization will be enormous. Even looking at the in-scope systems might lead to such data deluge. No organization will likely "fix" all of the problems; some kind of prioritization will have to occur. Various estimates indicate that even applying a periodic batch of Windows patches ("black" Tuesday) often takes longer than a period between patch releases (longer than one month). Accordingly, there is a chance that the organization will not finish the previous patching round before the next one rushes in. To intelligently prioritize vulnerabilities for remediation, you need to take into account various factors about your own IT environment as well as the outside world. Those include:

- Specific regulatory requirements (i.e., fix all medium- and high-severity vulnerabilities as indicated by the scanning vendor)
- Vulnerability severity for the environment (i.e., fix all vulnerabilities on in-scope systems)
- Related threat information and threat relevance (i.e., fix all vulnerabilities on the frequently attacked systems)
- Business value and role information about the target system (i.e., address vulnerabilities on high-value critical servers)

A new standard was proposed to classify vulnerability severity and unify such vulnerability prioritization efforts. The Common Vulnerability Scoring System (CVSS) (http://www.first.org/CVSS) takes into account various vulnerability properties such as priority, exploitability, and impact, as well as multiple local site-specific properties. The CVSS scheme promises to provide a uniform way of scoring vulnerabilities, as soon as more vulnerability information providers adopt it. When the standard matures, it has a good chance of showing up in various regulations, such as PCI, as well as voluntary "best practices" frameworks, such as ISO270001.

The next phase of mitigation is important in many environments where immediate patching or reconfiguration is impossible, such as a critical server running unusual applications. Despite the above, in some cases, when a worm is out or a novel attack is being seen in similar environments, protecting such a system becomes unavoidable. In this case, one immediately needs to do something to mitigate the vulnerability temporarily. This step might be performed by a host or network intrusion prevention system; sometimes even a firewall blocking a network port will do. The important question here is choosing the best mitigation strategy, which will also not create additional risk by blocking legitimate business transactions. However, since we have all of the relevant threats, vulnerability, and business context information, we can make the right decision about how to apply the shielding.

In this context, using anti-virus and intrusion prevention technologies might be seen as part of vulnerability mitigation, since these technologies help protect companies from the vulnerability exploitation (either by malware or human attackers).

Ideally, all vulnerabilities are fixed, such as patched or remediated in some other way in the order prescribed by the above prioritization procedure and taking into account the steps we took to temporarily mitigate the vulnerability above. In a large environment, it is not simply the question of "let's go patch the server." Often, a complicated workflow with multiple approval points is required.

To make sure that vulnerability management becomes an ongoing process, an organization should monitor the vulnerability management process on an ongoing basis. This involves looking at the implemented technical and process controls aimed at decreasing risk. Such monitoring goes beyond vulnerability management into other security management areas. It is also important to be able to report to senior management about the progress.

It should be added that vulnerability management is not a panacea even after all the "known" vulnerabilities are remediated. "Zero-day" attacks, which use vulnerabilities with no resolution publicly available, will still be able to cause damage. Such

cases need to be addressed by using the principle of "defense in-depth" during the security infrastructure design.

Now we will walk through all the requirements in PCI DSS guidance that are related to vulnerability management. We should note that vulnerability management guidance is spread across Requirements 5,6, and 11.

Requirement 5 Walkthrough

While anti-virus solutions have little to do with finding and fixing vulnerabilities, in PCI DSS they are covered under the umbrella definition of vulnerability management. One might be able to argue that anti-virus solutions help when a vulnerability is present and is being exploited by malware. Thus, anti-virus tools do help mitigate the consequences of exploited vulnerabilities in some scenarios.

Requirement 5 mandates the organization to "use and regularly update anti-virus software or programs." Indeed, many anti-virus vendors moved to daily (and some to hourly) updates of their virus definitions. Needless to say, a virus protection software is next to useless without an up-to-date malware definition set.

Unfortunately, PCI, as most compliance mandates, takes a "blast from the past" view of things by saying that "many vulnerabilities and malicious viruses enter the network via employees' e-mail activities." While this was very true in the 1990s and early 2000s, nowadays most malware enters a system through the Web browser. Internet Explorer is a primary culprit here; Mozilla Firefox malware is not out of question either.

PCI creators wisely chose to avoid the trap of saying "anti-virus must be on all systems," but instead chose to state that "anti-virus software must be used on all systems commonly affected by viruses to protect systems from malicious software." Somebody who is slightly out of touch with the current threat landscape might ask about those "systems commonly affected by viruses." The requirement further explains that "systems commonly affected by viruses typically do not include UNIX-based operating systems or mainframes."

Subsection 5.1.1 states that one needs to "ensure that anti-virus programs are capable of detecting, removing, and protecting against other forms of malicious software, including spyware and adware." They spell out all of the detection, protection, and removal of various types of malicious software, knowing full well that such protection is desirable, but not really achievable, given the current state of malware research. In fact, recent evidence points that guaranteeing that an anti-virus product

will protect you from all the malware, is becoming less certain every day as more backdoors, Trojans, rootkits, and other forms of malware enter the scene, where virus and worms once reigned supreme.

Finally, Section 5.2 drives the point home: "ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs." This combines three different requirements, which are sometimes overlooked by organizations that deployed anti-virus products. First, they need to be current—updated as frequently as their vendor is able to push updates. Daily, not weekly or monthly, is a standard today. Second, if you deploy a virus protection tool and then the virus or even an "innocent" system reconfiguration killed or disabled the security tool, no protection is present. Thus, security tools running status need to be monitored. Third, as mentioned in Chapter 6, audit logs are critical for PCI compliance. This section reminds PCI implementers that anti-virus tools also need to generate logs, and such logs need to be reviewed in accordance with Requirement 10.

Requirement 6 Walkthrough

Another requirement of PCI covered under the vulnerability management umbrella is Requirement 6, which covers the need to "develop and maintain secure systems and applications." Thus, it touches vulnerability management from another side: making sure that those pesky flaws and holes never appear in software in the first place. At the same time, this requirement covers the need to plan and execute a patch management program to assure that, once discovered, the flaws are corrected via software vendor patches or other means.

Thus, one finds two types of requirements in Requirement 6: those that help you patch the holes in commercial applications, and those that help you prevent holes in the in-house developed applications. Specifically, it states that "All systems must have the most recently released, appropriate software patches to protect against exploitation by employees, external hackers, and viruses."

To address a need to carefully test patches to avoid causing bigger problems than those that are being addressed, PCI DSS states that "appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations."

As mentioned above, the prescribed way of dealing with vulnerabilities in custom, homegrown applications, lies in careful application of secure coding techniques and incorporating them into a standard software development lifecycle.

Specifically, the document says that "for in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques."

Apart from requiring that organizations "ensure that all system components and software have the latest vendor-supplied security patches installed," Requirement 6.1 attempts to settle the debates in security industry: one between a need for prompt patching in case of an imminent threat and a need for careful patch testing. They take the simplistic approach of saying that one must "install relevant security patches within one month of release." Such approach, while obviously "PCI-compliant," might sometimes be problematic: one month is way too long in case of a worm outbreak (all vulnerable systems will be firmly in the hands of the attackers) and, on the other hand, too short in case of complicated mission-critical systems and overworked IT staff.

Further, Requirement 6.2 prescribes "establishing a process to identify newly discovered security vulnerabilities." Note that this doesn't mean "scanning for vulnerabilities" in your environment, but looking for newly discovered vulnerabilities via vulnerability alert services (some of which are free, while others, that can be customized to only send alerts applicable to you environment, are not). One can also monitor the public mailing lists for vulnerability information, which usually requires a significant time commitment.

Other aspects of your vulnerability management program apply to securing the software developed in-house. Section 6.3 states that one needs to "develop software applications based on industry best practices and incorporate information security throughout the software development life cycle." The unfortunate truth, however, is that there is no single authoritative source for such security "best practices" and, at the same time, current software "industry best practices" rarely include "information security throughout the software development life cycle." Thus, this requirement is somewhat conflicting. In detail, Section 6.3 goes mostly over software maintenance guidelines, such as:

6.3.1	Testing of all security patches and system and software configuration changes before deployment
6.3.2	Separate development, test, and production environments
6.3.3	Separation of duties between development, test, and production environments
6.3.4	Production data PANs are not used for testing or development

6.3.5 Removal of test data and accounts before production systems become active

6.3.6 Removal of custom application accounts, usernames, and passwords before applications become active or are released to customers

6.3.7 Review of custom code prior to release of production or customers in order to identify any potential coding vulnerability.

Among those, Section 6.3.4, "production data (live PANs) are not used for testing or development," is one that is the most critical and also the one most commonly violated with the most disastrous consequences. Many a company found its data stolen, because their developers moved the data from the more secure production environment, to a much less protected test environment, as well as on mobile devices (laptops), remote offices, and so forth.

The opposite, contaminating the production environment with test code, utilities, and accounts, is also critical (and was known to lead to just as disastrous compromises of production data), and is covered in Sections 6.3.5 and 6.3.6, which regulate the use of "test data and accounts" as well as pre-release "custom code."

Overall, paying attention to Section 6.3 will save an organization from a lot of pain in the future.

Further, Section 6.4 covers a critical area of IT governance: change control. Change control can be considered a vulnerability management measure, since unpredicted, unauthorized changes often lead to opening vulnerabilities in both custom and off-the-shelf software and systems. It states that one must "follow change control procedures for all system and software configuration changes," and even helps the organization define what the proper procedures must include:

6.4.1 Documentation of impact

6.4.2 Management sign-off by appropriate parties

6.4.3 Testing of operational functionality

6.4.4 Back-out procedures

Most other IT governance frameworks such as COBIT (www.isaca.org/cobit) or ITIL (www.itil.co.uk/) cover change control as one of the most significant areas that directly affect system security. Indeed, having documentation and sign-off for changes as well as an ability to "undo" things, will help to achieve both security and operations goals by reducing the risk, and striving towards operational excellence.

Section 6.5 covers Web applications, because it is the type of application that will be more likely developed in-house. Fewer organizations will choose to write their own software from scratch, compared to those creating or customizing Web application frameworks.

Requirement 6.5 points towards the Open Web Application Security Project (OWASP) project as a source of secure coding guidance. OWASM "Secure Coding Principles" (see www.owasp.org/index.php/Secure_Coding_Principles) covers the issues leading to OWASP Top Ten Web Application Security Issues (www.owasp.org/index.php/OWASP_Top_Ten_Project). In addition, it also calls to "review custom application code to identify coding vulnerabilities." While a detailed review of secure coding goes much beyond the scope of this book, there are multiple other books devoted to the subject.

PCI DSS goes into great level of details here, covering common types of coding-related weaknesses in Web applications. Those are:

6.5.1	Invalidated input
6.5.2	Broken access control (e.g., malicious use of user IDs)
6.5.3	Broken authentication and session management (use of account credentials and session cookies)
6.5.4	Cross-site scripting (XSS) attacks
6.5.5	Buffer overflows
6.5.6	Injection flaws (e.g., Structured Query Language (SQL) injection)
6.5.7	Improper error handling
6.5.8	Insecure storage
6.5.9	Denial of Service (DoS)
6.5.10	Insecure configuration management

In addition to secure coding to prevent vulnerabilities, organizations might need to take care of the existing deployed applications by looking into Web application firewalls. An interesting part of Requirement 6.6 is that PCI DSS recommends either a code review ("having all custom application code reviewed for common vulnerabilities by an organization that specializes in application security") or a Web firewall ("installing an application layer firewall in front of Web-facing applications"), completely ignoring the principal of layered defense or defense-in-depth.

Requirement 11 Walkthrough

Let's walk through the entire Requirement 11 to see what is being asked. First, the requirement name itself asks users to "Regularly test security systems and processes," which indicates that the focus of this requirement goes beyond just buffer overflows and format string vulnerabilities from the technical realm, but also includes process weaknesses and vulnerabilities. A simple example of a process weakness is using default passwords or easily guessable passwords (such as the infamous "password" password). It is interesting to note that the above process weaknesses can be checked from the technical side, such as during the network scan by a suitable scanner with password check enabled. However, another policy weakness, requiring overly complicated passwords and frequent changes, which in almost all cases leads to users writing the password on the infamous yellow sticky notes, cannot be "scanned for" and will only be revealed during an annual penetration test by a pentest team.

Later, the requirement text goes into a brief description of vulnerabilities in a somewhat illogical manner: "Vulnerabilities are being discovered continually by hackers and researchers, and being introduced by new software." Admittedly, vulnerabilities are being introduced first and then discovered by researchers (which are sometimes called "white hats") and attackers ("black hats").

The requirement then calls for frequent testing of software for vulnerabilities: "Systems, processes, and custom software should be tested frequently to ensure security is maintained over time and with any changes in software." An interesting thing to notice in this section is that they explicitly call for testing of systems (such as operating systems software or embedded operating systems), processes (such as the password management process examples referenced above), and custom software, but don't mention the commercial off-the-shelf (COTS) software. One can hypothesize that this is included as part of the system, since it is not only the operating system code, but vendor application code contains vulnerabilities. Today, most of the currently exploited vulnerabilities are found in applications such as MS Office, and, at the same time, there is a relative decrease of weaknesses in core Windows system services.

The detailed requirement start from Requirement 11.1, which mandates the organization to "test security controls, limitations, network connections, and restrictions annually to assure the ability to adequately identify and to stop any unauthorized access attempts." This requirement is the one that calls for an in-depth annual security assessment. Note that this assessment of controls is not the same as either a vulnerability scan or a penetration test. Obviously, if your organization is already

doing more rigorous security testing, there is no need to relax it to once per year. Also notice the list of "controls, limitations, network connections, and restrictions," which again covers technical and non-technical issues. The term "controls" is broad enough to cover technical safeguards and policy measures.

In addition, wireless network testing is spelled out: "use a wireless analyzer at least quarterly to identify all wireless devices in use." Indeed, the retail environment of 2007 makes heavy use of wireless networks in a few common cases where POS wireless network traffic was compromised by the attackers.

Further, Section 11.2 requires one to "run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades)." Even though many grumble that "after any changes" is not clear enough (after all, one would not scan the entire enterprise network after changing a single rule on a router somewhere deep in the test environment), this requirement does catch both needs to assess the vulnerability posture: periodically and after a change to make sure that new vulnerabilities and weaknesses are not introduced.

This requirement has an interesting twist, however. "Quarterly external vulnerability scans must be performed by a scan vendor qualified by the payment card industry." Thus, just using any scanner won't do: one needs to pick it from the list posted at the PCI DSS site (see https://www.pcisecuritystandards.org/resources/approved_scanning_vendors.htm). Specifically, the site says: "The PCI Security Standards Council has assumed responsibility for the Approved Scanning Vendor (ASV) program previously operated separately by MasterCard Worldwide. All new and renewing ASVs must enroll directly with the Council, as MasterCard has terminated its program as of October 27, 2006."

At the same time, the requirements for scans performed after changes are more relaxed: "Scans conducted after network changes may be performed by the company's internal staff." This is not surprising given that such changes occur much more frequently in most networks.

The next item, Requirement 11.3, covers penetration-testing requirements. It says: "Perform penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a Web server added to the environment)." The logic here is again similar: periodic (annual) and after major changes. It appears that in this case, the changes that trigger a penetration test should be of much large scale, since penetration tests aren't exactly cheap.

Moreover, PCI DSS dives deeper into penetration testing details. "These penetration tests must include the following:

11.3.1 Network-layer penetration tests

11.3.2 Application-layer penetration tests.

Indeed, limiting to network layer tests is shortsighted, but this list still leaves an amazing gap of non-technical penetration testing. Admittedly, most skilled penetration testing teams will perform such non-technical testing as well, but not mentioning it explicitly in PCI official documents seems like an oversight.

Further, the requirements deviate from vulnerability assessments, penetration testing, and other security testing and move into detection and protection technologies. Section 11.4 covers three such technologies: Network Intrusion Detection Systems (NIDSes), Host-based Intrusion Detection Systems (HIDSes), and Intrusion Prevention Systems (IPSes) (presumably, both host-based and network-based). In particular, it recommends to "use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises." However, one can understand that focus on the network traffic is somewhat limited. In fact, host-based IDS and IPS have little to do with network traffic, and mostly monitor and protect individual hosts. Even though some HIPS can control network traffic to and from the host (serving as a personal firewall), a major function of a HIPS is protection from malicious processes and attacks on the host itself.

PCI documents also do not forget a critical requirement for updating the above technologies: "keep all intrusion detection and prevention engines up-to-date." Indeed, a signature-based IDS or an IPS with an old signature set is not able to detect or block the newest attacks, and thus is not realizing its full potential.

Sometimes called "last layer of defense," file integrity checking technologies are also mandated by the PCI DSS guidance. Requirement 11.5 calls to "deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system or content files." Such software usually utilized cryptographic checksums to "fingerprint" the files.

PCI requirements also address one of the common questions of in-scope systems. Specifically, it states that " critical files are not necessarily only those containing cardholder data." Indeed, "for file integrity monitoring purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise," since a change of a system file on a pay-

ment processing server is no less critical than a change of the payment database itself. A server compromise will mean that all of the data on the system in question will be available to an attacker.

The PCI DSS applies to all system components. These components include all applications, databases, systems, network devices, firewalls, and so forth, that store, process, or transmit cardholder data. As a reminder, when we talk about cardholder data, we are specifically interested in the PAN (the card number on the front of payment cards). The cardholder data environment also includes any other systems that are connected to this network if they are not separated by a firewall or other network access controls/segmentation (even if they aren't involved in processing). This is why it is so important that the organization subject to the PCI DSS (e.g., merchant or service provider) properly segment its cardholder data systems and supporting infrastructure and then use this information to categorize the systems as in-scope or out of scope.

Common PCI Vulnerability Management Mistakes

It is also worthwhile to point out a few common mistakes that organizations make while working towards the Requirement 11 compliance. You should note that some of them are broader than just a Requirement 11.

We hinted at the first mistake when we described the password example. It is in focusing only on the technical assessment means (which are indeed easier and more automatic) and omitting the process-based mistakes. Thus, people often focus on the technical vulnerabilities and forget all of the human vulnerabilities, such as susceptibility of many enterprise IT users to social engineering, and other lapses of corporate controls. The way to avoid this mistake is to keep in mind that even though you use a scanning vendor, your credit card data might still be pilfered, and addressing the "softer" part of security is just as critical.

Another commonly lost thing is application-level vulnerabilities, which is not only about open ports and buffer overflows in server code. It is also about all the Web application (e.g., Cross Site Request Forgery) and client side applications (all the recent MS Office weaknesses that lean to many a government agency falling victims to hackers) What is in common across those "newer" vulnerability? Scanning for them is not as easy to automate as finding open telnet ports and overflows in Internet Information Services (IIS). PCI requirements refer to such weaknesses but,

still, more attention seems to be paid to the network-level stuff. The way to avoid this mistake is to keep in mind that a lot of hacking happens on the application layer.

Even when application-layer vulnerabilities are not forgotten, there is something else to be missed: vulnerability in the applications that were written in-house. Indeed, no vulnerability scanner vendor will have knowledge of your systems, and even if your pen-testing partner will be able to discover some of them during an annual penetration test, a lot of application code can be written in a year (and thus a lot more vulnerability introduced). The way to avoid this mistake it to train your software engineering staff to use secure programming practices to minimize the occurrence of such flaws. While having a good application pentester on staff is unlikely, assessing the security of the homegrown application needs to be undertaken more frequently than once a year.

The last mistake we mention is misjudging the list of in-scope systems. Indeed, modern large-scale payment processing systems are complicated and have many dependencies. Avoiding this mistake is not easy: the only way to find all the systems that might need to be scanned and protected is to have your internal staff (who know the systems best) work with an external PCI consultant (who knows the regulation best) to find out what should be in scope for your particular environment.

Keeping these mistakes in mind has the chance of making your PCI compliance experience a lot less painful.

Case Studies

The case studies below illustrate how vulnerability management for PCI is implemented in a few real-world organizations.

PCI at a Retail Chain

This case study covers how PCI Requirement 11 was dealt with at a large retain chain in US Midwest. The Unnamed Retailer, Inc. did not perform any periodic network vulnerability scanning and didn't employ the services of a penetration-testing firm. Their IT security staff sometimes used the freeware tools to scan a specific system for open ports or sometimes for vulnerabilities, but all such efforts were ad hoc and not tied to any program.

Upon the approach of PCI compliance deadline, the company had to start the scanning using the PCI-approved scanning vendor every quarter. They chose to

deploy a service-based vulnerability scanning from a major vendor. The choice of vendor was determined after a brief proof-of-concept study.

Initially, they suffered from having no information or no knowledge of their vulnerability posture to having too much, since they decided to scan all the Internet-facing systems. Later however, they reduced the scope to what they considered to be "in-scope" systems such as those processing payments (few of those systems are ever visible from the internet, however) and those connected to such systems.

Later their scanning vendor introduced a method to scan the internal systems, which was immediately utilized by the retailer. However, it turned out that finding which internal systems are in-scope is even more complicated, since many systems have legitimate reasons to connect to those that process credit card transactions. For example, even their internal patch management system was deemed to be in-scope, since it frequently connected to the transaction processing servers.

As a result, their route to PCI vulnerability management nirvana took a few months following a phased approached. Implementation followed the following route:

1. All Internet-facing systems that can be scanned
2. A smaller set of Internet-facing systems that were deemed to be "in-scope"
3. A set of internal systems that either process payments or connect to those that do
4. From there, the company will probably move to scanning select important systems which are not connected to payment processing, but are still critical in their business.

Even though the organization chose not to implement the intrusion detection earlier, their PCI auditors strongly suggested that they look at some options in this area. The company chose to upgrade their firewalls to Unified Threat Management (UTM) devices that combined the capabilities of a firewall and a network IPS. An external consultant suggested their initial intrusion prevention rule set, which the company deployed.

Overall, the project ended up with a successful, if longish, implementation of PCI Requirement 11 by using a scanning service as well as UTM devices in place of their firewalls. The organization did pass the PCI audit, even though they were told to also look at deploying a file integrity monitoring software, which is offered by a few commercial vendors.

PCI at an E-commerce Site

This case study is based on a major e-commerce implementation of a commercial scanning service, a penetration testing by a security consultancy, and a host IPS and file integrity monitoring on critical servers.

Upon encountering PCI compliance requirements, Buy.Web, Inc. has assessed their current security efforts, which include the use of host IPS on their demilitarized zone (DMZ) servers as well as periodic vulnerability scanning. They realized that they needed to additionally satisfy the pen testing requirements as well as file integrity checking requirements to be truly compliant. Their IT staff performed an extensive research of file integrity monitoring vendors, and chose one with the most advanced centralized management system (to ease the management of all the integrity checking results). They also contracted a small IT security consultancy to perform the penetration testing for them.

The team also utilized their previously acquired log management solution to aggregate the host IPS and file integrity checking, to create a single data presentation and reporting interface for their PCI auditors.

Overall, this project was a successful illustration of a mature security program that needed to only "fill the gaps" to be PCI compliant.

Summary

To conclude, PCI DSS document covers a lot of activities related to software vulnerabilities. Let us summarize what areas are covered, since such requirements are spread over multiple requirements, even belonging to multiple sections.

Vulnerability-related activity prescribed by PCI DSS	Requirement
Secure coding guidance in regular and Web applications	Requirement 6
Secure software deployment	Requirement 6
Code review for vulnerabilities	Requirement 6
Vulnerability scanning	Requirement 11
Patching and remediation	Requirement 6
Technologies that protect from vulnerability exploitation	Requirement 5, Requirement 6, Requirement 11
Site assessment and penetration testing	Requirement 11

As a result, PCI allows for comprehensive, if a bit jumbled, look at the entire vulnerability landscape, from coding to remediation and mitigation.

Solutions Fast Track

Vulnerability Management is in Many Places in PCI

☑ Make sure that you look for all vulnerability-related guidance while planning your PCI-driven vulnerability management program

Remember That Vulnerabilities Occur Not Only in Operating System Software

☑ Assess the vulnerability of business applications

☑ Do not forget custom applications written in-house or by partners

Remember That Vulnerability Management is Not Only About Assessment

- ☑ Have an ongoing program to deal with discovered vulnerabilities
- ☑ Automate the remediation of discovered vulnerabilities
- ☑ Make sure that you recheck for fixed vulnerabilities after they are reported to be fixed

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to **www.syngress.com/solutions** and click on the **"Ask the Author"** form.

Q: If I use a vulnerability scanner, am I OK in regards to PCI?

A: Maybe, but most likely not. Scanners can discover vulnerabilities, but can do little to actually fix the vulnerabilities; you need to do this work based on the scan results.

Q: How can I prove to PCI auditors that I am "compliant" with Requirement 6?

A: Demonstrating that you have a program to prevent, discover, and remediate code and configuration weaknesses should provide ample proof that you are taking Requirement 6 seriously.

Q: How do I assess my custom Web applications for vulnerability if my scanner doesn't have a check for them?

A: First, dedicated products exists to assess custom Web application security. In addition, having source code to your own Web applications helps to discover and fix vulnerabilities from the code side.

Chapter 9

Monitoring and Testing

Solutions in this chapter:

- **Monitor and Test**
- **Monitor and Track (Audit) Network and Data Access**
- **Periodically Test Systems (and Processes)**

Introduction

Generally speaking, the best approach to any industry or government regulatory requirement has been to find a middle ground in terms of effort and cost to meet the spirit of the requirement, and then work with the auditor ahead of audit time to see how you've done. Generally, that approach reaps rewards that pay off in reduced "patching" of the effort. Obviously, meeting with the auditor before you start makes a lot of sense, but making certain the results meet with the auditor's approval is where your Return on Investment (ROI) will show up. If the auditor is happy, then the card issuer will be happy.

This is certainly true where Requirements 10 and 11 of the Payment Card Industry (PCI) requirements come into play. Requirement 10, Monitoring, and Requirement 11, Testing, are easily capable of inflating PCI compliance costs to the point of consuming the small margins of card transactions. No one wants to lose money to be PCI compliant. Therefore, the ability to meet the requirements above all must make business sense. Nowhere else in PCI compliance does the middle ground of design philosophy more come into play than in the discipline of monitoring, but this is also where minimizing the risk can hurt most.

Monitoring Your PCI DSS Environment

PCI Data Security Standard (DSS) Requirement 10 states: "Track and monitor all access to network resources and cardholder data". The requirement around monitoring is potentially broad and far-reaching, but there are boundaries to be determined, and that is the first, best step an Information Technology (IT) architect or engineer can take in determining the boundaries.

A PCI compliant operating environment is where the cardholder data exists. That data can never be allowed out of that environment without knowledge by way of auditable logging. Assuming you've designed your PCI environment to have appropriate physical and logical boundaries (through use of segregated networks and dedicated applications space), you should be able to identify the boundaries of your monitoring scope. If you haven't done this part, go back to Requirement Number 1 and start over!

Once your boundaries are determined, it's time to start digging into the details.

Establishing Your Monitoring Infrastructure

When an architect or engineer goes about designing a computer environment, he or she will be aware of basic components in the form of capabilities that enable functionality at the various layers of the network. These are the things that make Internetworking of computer platforms possible across hubs and switches and routers. These are also the things that make monitoring of these networked components reliable. It is reliability that makes for a well-constructed monitoring solution that will stand the test of an audit, and survive scrutiny in a courtroom (should that necessity arise).

Any successful operating environment is designed from the ground up, or, in the case of a networking infrastructure and applications space, from the wires on up. It's important, therefore, to plan your monitoring of your PCI compliant operating environment the same way you designed it. But to play in this environment you need basic components you cannot do without.

Time

During early development of computer networks, scientists discovered quickly that all systems had to have a common point of reference to develop context for the data they were handling. The context was obviously a reliable source of time, since computer systems have no human capacity for cognitive reconstruction or memory. The same holds true today for monitoring systems. We would all look a bit foolish troubleshooting three-week-old hardware failures, so hardware monitoring had it right from day one. It seems fairly straightforward that time and security event monitoring would go hand in hand.

PCI requirement 10.4 states that the source for time in your environment must be configured for acquiring time from specific sources. Good monitoring systems (event management, network intrusion prevention) and forensic investigation tools rely on time. System time is frequently found to be arbitrary in a home or small office network. It's whatever time your server was set at, or if you designed your network for some level of reliance, you're systems are configured to obtain time synchronization from a reliable source, like the Naval Observatory Network Time Protocol (NTP) servers (see http://tycho.usno.navy.mil/ntp.html).

Subsequent network services on which a PCI compliant environment would rely include Domain Name System (DNS), directory services (such as Sun's or Microsoft's), and Simple Mail Transfer Protocol (SMTP) (e-mail). Each of these in

turn rely on what are referred to as "time sources." Stratum 1 time sources are those devices acquiring time data from direct sources like the atomic clocks run by various government entities or Global Positioning System (GPS) satellites. Local hardware, in fact, is considered Stratum 1; it gets time from its own CMOS. Stratum 2 gets their time from Stratum 1, and so on.

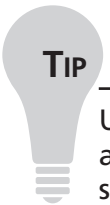
For purposes of PCI compliance, Stratum 2 is typically sufficient to "prove" time, as long as all systems in the PCI environment synchronize their clocks with the Stratum 2 source. Of course, PCI does not say anything about time synchronization. So what's the big deal?

Event management. That's the big deal. Oh, and PCI Requirement 10.4, too.

Here's the rub: What is your source for accurate time? How do you ensure that all your platforms have that same reference point so the event that occurred at 12:13 P.M. GMT is read by your event management systems as having occurred at 12:13 P.M. GMT instead of 12:13 A.M.?

There are two facets to the approach. One is to make sure you have a certified source of time into your environment (see: http://tf.nist.gov/service/time-servers.html for a list of stratum 1 sources of time). Second is to make sure you have the means to reliably replicate time data across your network.

Stratum 2, as mentioned, is an acceptable source for your monitoring environment, and that data can be acquired via the Internet from the National Institute of Standards & Technology (NIST) sources as described in the text. By using a durable directory service, the time data can be advertised to all systems, assuring no worse than a 20-second skew. In an Active Directory forest, for example, the Primary Domain Controller (PDC) emulator serves as a Stratum 2 source. Servers in the forest operating the parameters of W32Time service (based on Simple Network Time Protocol [SNTP]) adhering to RFC 2030, can therefore provide adequate time synchronization to within 20 seconds of all other servers in the AD forest.



TIP

Using a Stratum 1 source for time into your environment is not necessary for a business. Large enterprises use Stratum 1 sources (such as GPS satellites) but spend a lot of money to do it. Stratum 1 time acquisition is accomplished by using technology from companies like Symmetricom (http://www.ntp-systems.com/), who produce NTP solutions around an appliance. The appliance itself would have to be wired to a satellite antenna that is then mounted on the roof of your data center or other facility. It's an expensive solution.

Obviously, having reliable power and network is critical to this sort of approach, but it's fairly easy to overlook. When you're planning for PCI compliance, who looks at the clocks?

Active Directory servers can be configured as authoritative time servers. Read this technical article from Microsoft (http://support.microsoft.com/kb/816042) to find out how.

Identity Management

One might suppose that the basics of any infrastructure mandate a good identity management solution, perhaps based on Microsoft Active Directory or Novell eDirectory. Just like "Time," PCI DSS does not say much about how you implement, only that you have a solution.

Identity management solutions can be configured to have multiple roles per identity and multiple identities per user. It's important, therefore, to sort out how you need your solution to behave in the context of your card transaction environment. Roles-based identity has never been more difficult; therefore, many different industry and government regulations and standards call for them. Separation of duties is a concept that pervades throughout every business.

Choosing the directory solution has everything to do with which platforms will operate in your environment. Either train or hire strong engineering and architectural staff to make sure this solution is deployed without a hitch. This text is not a discourse on identity solutions, but this is a worthwhile point.

To bring a robust identity structure to your card transaction environment, first, make sure the identity solution has its own instance within the card transaction environment. This might constitute a dedicated Lightweight Directory Access Protocol (LDAP) organization (or Active Directory domain), such as pos.acme.com, which would be a subdomain of acme.com. Second, apply appropriate security settings to your directory.

Security settings should be configured to basically track all access to systems in your directory domain. That is a good reason for having a dedicated domain in the first place; here, there are no safe systems and no assumptions of innocence. All access is tracked for audit.

The system logs are sent to the event management solution immediately for correlation and archival. No opportunity for alteration must exist!

Establish the roles within the monitoring environment. There are really only two: system administrators and security log administrators. That's it. No one else should set foot (or network interface card [NIC]) in that environment. Make sure the system administrators are not the same lot that manage your PCI network if you can help it.

Each ID must be audited in much the same manner as within your PCI environment. Log each access. Each identity associated with your log monitoring environment must have a person attached to it. No *guest* IDs, no *test* IDs.

Event Management Storage

Keeping the facility that captures and stores your logs happy is paramount to your ability to maintain PCI compliance. Logs add up quickly when you consider your sources:

- Firewalls
- Switches
- Servers
- Applications
- Databases
- IDS
- Other Security Software such as Antivirus

The amount of data a business deals with in this space can easily reach into the terabytes. Good thing disk space is so cheap! (Relatively speaking, of course, tools that handle and correlate this data might not be so cheap.)

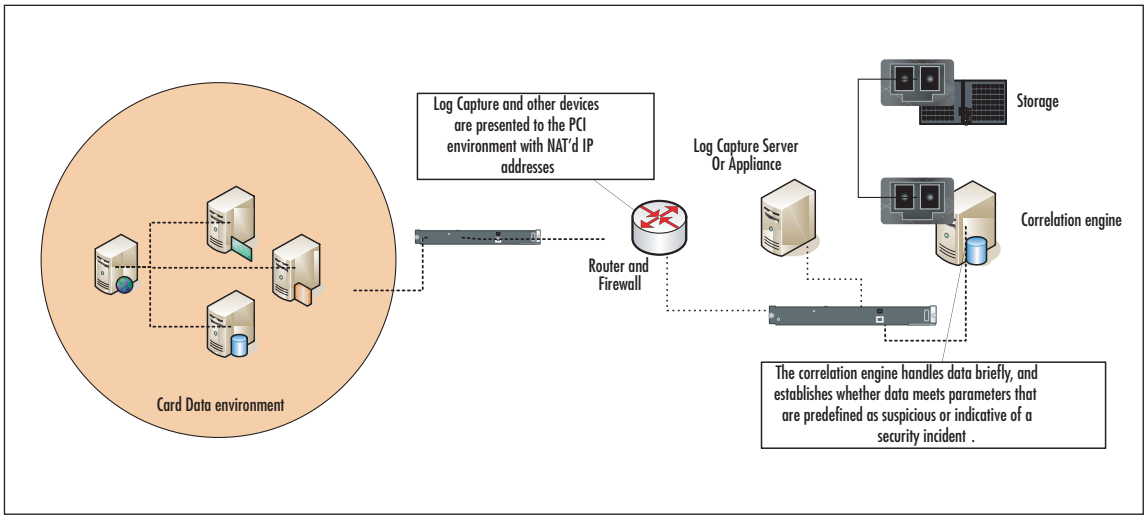
Using Storage Area Network (SAN) technology is the best way to go in terms of storage. You might consider Direct Access Storage Device (DASD) connected to the various servers that handle log transfer, but what if you're dealing with appliance-based solutions? What if you're dealing with a combination?

SAN is really the best way to go for a hybrid- (appliance and server) based solution. You need this data in a reliable, separate architecture where it can exist for a long time (up to a year) and can be recalled on short notice (such as after a security incident).

Where all of this data will live is a bit different from where it will be stored. Storage can be connected to the appliances and servers via fiber channel either directly to a fiber channel (FC) card, or over the Internet Protocol (IP) network (see

Figure 9.1). Accessing that data, therefore, can be different. The storage of the old data is not relevant to dashboards and alerting systems, but is more relevant to audits. The live or current data, therefore, may be stored closer to the correlation systems than the archive data.

Figure 9.1 Connecting Storage Devices.

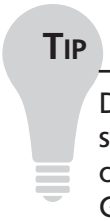


The enormous amount of data you will deal with in the course of logging and monitoring your environment means you must keep abreast of your available storage space and fabric capacity. As mentioned earlier, storage disk may be cheap, but acquiring EMC or other brands of SAN devices can be costly. Forecast your needs and have good capacity planning processes in hand!

As far as handling and then alerting on this data, you will need to select from a small population of security event/incident vendor technologies that automate this daunting task. The number of requirements you use during the selection process is significant.

Does the vendor support all your operating systems? Applications? Security tools?

Develop your list of requirements, then start shopping. Deploying a security event management solution is critical to your success and will help you meet PCI DSS 10.6.



TIP

Don't be fooled by every magazine you pick up from the shelf at the book store. Selecting a good storage solution is a huge undertaking, because the costs can be high if you choose poorly. Refer to reports by groups such as Gartner (www.gartner.com) or Forrester (www.forrester.com) to understand where the market for such technologies are headed, which company has the best management tools, and which company is most viable.

Nothing hurts an IT investment more than hanging your hat on a company that goes bankrupt six months after you signed the purchase order.

Determining What You Need to Monitor

Knowing what you are monitoring is half the battle in planning your storage needs as well as successfully deploying an auditable PCI-DSS solution. Any well-intentioned system administrator can tell you the basic equations to develop the amount of storage needed for a firewall or a Network Intrusion Detection System (NIDS) device. It cannot be stressed enough, however, that trapping all that is log-able is *not* the point. To do so would be counterproductive. The fact of PCI-DSS as protection of cardholder data is paramount, and therefore should be the focus of all logging activity.

To this point, it is time to examine what exactly we are required to monitor.

Applications Services

It's best to break up the task of monitoring and logging into two less daunting components. Best because the activity you are performing had best not interfere with the primary job of the components you're monitoring, which is providing services to merchants (i.e., serving up cardholder information to a point of sale and to a financial institution).

Monitoring tools are meant to be unobtrusive, exhibiting a small resource footprint on their hosts and networks; if you overwhelm either, card transactions can be impacted. This would obviously be an undesirable situation that can create significant financial burdens and sudden career changes.

In this respect, we have grouped the "Application Services" of data storage and access. These systems are the honey of the hive, and are the point of aspiring to PCI compliance. This is our primary goal as well as that of any hacker looking for some data of return value.

Data Storage Points

Storage of cardholder data is a necessary evil. During the course of business, a point-of-sale solution must make fast transactions possible to approve or deny sales to a cardholder.

The storage points must be protected by a number of solutions, and typically are hosted on servers of some sort. Intrusion detection (such as TripWire), intrusion prevention, antivirus, and system logs are all sources of auditable data that must be captured and transmitted to your security event management solution.

Data Access Points

So, you have cardholder data inbound and outbound via a e-commerce system, some is being stored, some is being sent on to a financial institution, some is being sent back to your point-of-sale system in the form of acknowledgements, approvals, denials, take-the-card notices, and so on. How do you know that only *your* systems are able to see that data? How do you know that no other entity is intercepting or otherwise recording these data streams?

Of course, the users of the systems between POS and the bank are all accounted for and their access is logged and monitored. To make certain no hackers have gained access to these "supply chain" systems, the access of the systems is logged, best done via system logging (e.g., Windows-family servers event logging). Microsoft has published a paper regarding logging of privileged access, which can be found at http://support.microsoft.com/kb/814595 . Active Directory is an infrastructure component, and is frequently leveraged to grant access to applications resident on Windows Server hosts. As such, the access to the host is logged as well as access to the application.

Application logs can also be acquired using technology tailored to the task. Tools such as CA's Unicenter WSDM (for Windows platforms) and Oracle's WS-Security can be configured to acquire logs, then transfer them to your security event management solution.

Here, the point will be repeated; the logs will be moved to the event management solution for archival; no opportunity for alteration exists!

Infrastructure Components

The Infrastructure is the carrier and handler of the cardholder data. Operating systems and the management tools that support them do not care nor do they understand the financial transactions that are occurring around them. Therefore, the code

that runs on these components is necessarily low-level. We don't anticipate a Microsoft MOM agent to understand a Simple Object Access Protocol (SOAP) transaction, only its impact on central processing unit (CPU) and memory input/output (I/O).

Because of this, it is a safe assumption to make that this area is at least as important, if not more so, to watch with strong monitoring and alerting systems. It's also easier to overdo the solution, and impact the mission-critical services above. No matter how mission critical and infrastructure components are viewed, the care and feeding of one must not overwhelm the functionality of the other.

Infrastructure, by not having a good sense of what's happening at the applications layer, is an ideal place for a hacker to set up camp and search for good data of the sellable sort. A hijacked operating system or worse, a sniffer planted on the network by an insider, is a sure means of gathering such data.

Host Operating Systems (aka Servers)

The host operating system is probably the trickiest bit of the puzzle. Too many people have access to it, no matter how far you lock it down. There are system administrators, security administrators, and of course backup/restore folks. Each of these roles need to have a level of access, however, at no point should these folks be able to alter the system logs.

This is where Security Information Management (SIM) becomes quite handy in the area of system lockdown. When configuring the host, install a SNARE agent on it. Configure the agent to send the host system logs to your log collector. Also, configure the host to not retain logs for longer than 48 hours locally.

By configuring the host in this fashion, you have some local log data that is valuable to your administrators for technical reasons, but you've also moved the log data to a remote location. You've made it impossible for a hacker to cover his tracks.

A very important point: don't just move the logs then deleted them locally. Your system administrators and other support staff need these logs as well.

Network Objects

Wired and wireless. Routers, switches, hubs. Firewalls. Each of these components provide for intercommunication between and within networks. Each also generates logs of various levels of detail and size. Configure these platforms to send logs to your SIM solution.

Usually, you're not going to be able to load software on a supervisor card to route traffic logs; that's not how it works. You need skilled networking people to configure your infrastructure to send SNMP 2.0-compliant data to your SIM solution. The SIM will handle what it can in terms of load. This is where significant planning of your SIM solution comes into play.

The SIM itself must be *very* scalable if you're dealing with a large network with many subnets or bridged environments. The traffic is valuable to the correlation activities, so you want to capture as much of it as you can. That means you need a log collector proximate to your heaviest log-generating locations. Typically, a nexus of your network activities.

WARNING

Wireless networks are really a bad way to conduct business securely; nevertheless they are accepted as being a reality. PCI DSS 1.1 requires that a wireless operating environment be physically segregated from a wired environment and appropriately firewalled. It's a good thought, but let's face it, if someone can get into your wireless network, then it's not too much of a leap to get into the wired one. Therefore, using a strong wireless access monitor (see the "Solutions" section below) is critical to controlling your environment.

One would be surprised at the number of vending machines that accept credit cards and use wireless connectivity to transmit the transaction!

Wireless security is still very immature, so bulletproof security measures are not achievable. You can take every precaution to give your environment a modicum of security from wireless hacks, but you will still be vulnerable. Proof of this can be seen in what happened to TJX Companies (owner of TJMaxx). Their wireless network was leveraged by hackers to gain entry to cardholder data storage platforms. This resulted in an $8 million dollar gift card fraud scheme that has resulted in major lawsuits brought against TJX by the banks who have had to foot the bill for the fraud.

Determining How You Need to Monitor

What Gets Monitored

The simple statement "monitor everything" might be a wish in the dark for security professionals. After all, monitoring it all costs much more than the business might be

bringing in the door. The cash margins still take precedent, but the balance of security cost versus loss of prestige and associated business must be weighed. Within that balance, establish what budget can be assigned to monitoring, then figure out "What will hurt my business if it is compromised?"

Security Information Management

A SIM solution at its heart is nothing more or less than a log collector and its correlation engine. The log collector's role is to acquire the log, normalize it (that is, translate the log data into the schema used by the vendor), then pass it on to the correlation engine.

The correlation engine uses rules, signatures (though not always), and sophisticated logic to deduce patterns and intent from the traffic it sees originating at the host operating system (OS) and network layers. Well-designed SIM technologies try to distribute much of the "heavy lifting" in terms of moving data, but the actual analysis of that data *must* be centralized in some form.

A SIM solution must be scalable! In other words, wherever your business has data, you should have some central point where a log collector is going to have a reasonable chance of receiving your logs, then passing them on. If you have an important subsidiary that handles significant volumes of cardholder data, you don't want your log collector at a remote office. You need to have it near where the data flows and where it is stored.

Security Event Alerting

When a correlation engine has determined that something is amiss (see "Are you 0wned?"), it will attempt to alert your security team in whatever fashion you configured. Typically, this alert is via e-mail or pager, though some folks use Windows popup messenger, a Web-based broadcast message, a ticket sent to a response center, or even a direct phone call from the alerting system.

Whichever means you decide on, make sure you do not use just one part of your infrastructure to deliver that message. If your business uses Voice-over-IP (VoIP) for phone services, a well-crafted network attack could disable your phone services. If an e-mail solution is disrupted by a spam attack or a highly virulent e-mail worm, you might not be able to receive the data from your SIM solution.

Make certain you use two separate forms of communication to send alerts from your SIM to your security team.

Are You Owned?

Getting Tipped Off That You Have a BOT on the Loose

When intrusion detection systems (IDSes) are configured correctly, your security team has spent time understanding which systems are expected to send data and initiate communications, and in what fashion. For instance, a Web server is not expected to initiate port 80 communications if it is configured to only support Secure Sockets Layer (SSL) communications for the purpose of completing online purchase transactions.

Similarly, the Web server is not expected to initiate communications to a foreign IP address using a port that supports I Seek You (ICQ) traffic.

When IDS is configured correctly, your solution will detect such anomalies and alert you to their existence.

Deciding Which Tools Will Help You Best

Log Correlation

SIM tools provide incredible capabilities, and the best (and sometimes most questionable) include strong correlation capabilities. This means the system is able to acquire logs and events from disparate sources, normalize and compare the data presented, and make a logical deduction as to their meaning.

For instance, a series of calls outbound from a file server to an IP address over ICQ channels would tip off the SIM tools that a famous worm is running amok within the network. This in turn would generate an alert received by the Security Administrator, who then would have words with a certain System Administrator or two.

Log Searching

We'll cover the log searching tools in greater detail in the next section of this chapter, but a note about selection of this tool is worthwhile here.

Generally, a database should be searchable in the same manner by a variety of tools, but the fact is that many vendors spend less effort on their retrieval tools than on their correlation and storage components—that's a situation generated by market forces. PCI

DSS mandates an ability to retrieve data in much the same way as Sarbanes-Oxley (SOX) does. Therefore, SIM vendors have put more effort in the space.

If possible, using the *same* vendor for data retrieval is the best possible approach. However, if the retrieval capabilities show significant delay in reacquiring data (more than 24 hours), then consider another vendor. PCI DSS 10.6 gives some guidance in this area, but from a security perspective, a day is an eternity—the perpetrator is already gone.

Alerting Tools

Each vendor of SIM tools provides integration points to hook into sophisticated alerting systems. These take the form of management consoles that in turn provide SMTP, SNMP, and other means to transmit or broadcast information to whatever mode of communication is in play (e.g., pager, Smartphone, and so on).

Auditing Network and Data Access

The audit activities are proof of the work you've put into your PCI DSS solution. They help you understand where you are and how far you need to go to achieve nirvana. Or something similar. Fortunately, in this instance, the card issuers have helped us out in the form of the PCI DSS Security Audit Procedures (version 1.1, found here: www.pcisecuritystandards.org/pdfs/pci_audit_procedures_v1-1.pdf).

Searching Your Logs

Finding the best tool to mine log data after it has been archived (meaning, after it has been correlated and subjected to logic that detects attacks and such), is a very important bit of work. The point here is that after you've committed your terabytes of data to disk, you need a way to look for cookie crumbs if you've discovered an incident after-the-fact.

Data mining is a term normally associated with marketing activities. In this case, however, it's a valuable security discipline that allows the security professional to find clues and behaviors around intrusions of various sorts.

Some options for data mining include the use of the correlation tool you selected for security information management. In fact, most SIM tools now carry strong data mining tools that can be used to reconstruct events specific between IP and Media Access Control (MAC) identifiers.

The point is that the solution must be able to integrate at the schema layer. You don't want to invest in additional code just to make a data miner that typically looks for apples, to suddenly be able to look for oranges. If your current SIM vendor doesn't provide mining tools, insist on them, or take your business elsewhere.

Testing Your Monitoring Systems and Processes

Throughout this chapter, we have been preparing you to implement PCI DSS solutions covering each of the requirements. With diligence, skill, and just a little bit of luck, you have deployed a strong security solution that would meet the rigors of PCI DSS certification. Also, if done correctly, you will be ready to far exceed PCI DSS. Do not forget that the goal of PCI DSS is to create a framework for good security practice around the handling of cardholder data. It is *not* prescriptive security for the entirety of your IT infrastructure!

The activity of testing the PCI DSS environment, you might find, is actually quite straightforward. First you must find a good testing service. PCI DSS does not differentiate between what you do in-house and what is done for you by a third-party vendor, but the PCI group does provide a list of Approved Scanning Vendors (ASVs) that have been prescreened for their thorough processes and reporting. If you would rather not invest the significant dollars in creating your own penetration testing team, you would be well advised to scan the list of ASVs here: www.pcisecuritystandards.org/resources/approved_scanning_vendors.htm.

You also must engage a Qualified Security Assessor (QSA). The QSA is your auditor. This is the person who will actually walk through your test results and validate that your business is PCI DSS certifiable. The QSA is covered in Chapter 3.

Network Access Testing

The ASV will need full access to your network to perform the testing here. The idea is to expose the solutions you have deployed to appropriate testing. Whether it's possible or not, every egress and ingress must be examined for issues.

Penetration Testing

Every penetration test begins with one concept—*communication*. A penetration test is normally viewed as a hostile act. After all, the point is to break through active and passive defenses erected around an information system. Communication is important

because you're about to break your security. Typically, companies that do not approve a penetration test come down hard on the tester.

During the time of the penetration test, alarm bells will ring, processes will be put into motion, and, if communication has not occurred, and appropriate permissions to perform these tests have not been obtained, law enforcement authorities may be contacted to investigate. Now wouldn't that be an embarrassment if your penetration test, planned for months, had *not* been approved by your Chief Information Officer (CIO)?

Intrusion Detection and Prevention

Detection and prevention technologies have collided in recent months and are certain to converge to greater degrees over time. In the context of network and host activities, you should search for solutions and technologies where the best of breed is represented. Intrusion detection and prevention are more frequently housed on the same platform. This is an area where the business can see a better return in investment than on standalone solutions.

Intrusion Detection

Intrusion detection is a funny thing. Some focus on the network layer, some on the application layer. In a PCI DSS environment, you are typically dealing with application-layer traffic. Web services behaviors and transactions using eXtensible Markup Language (XML), SOAP, and so on. There are two sorts of IDS in this context: *network* and *applications*. In addition, there are two layers of IDS: *network* and *host*.

Network IDS is going to work in a similar vein to Intrusion Protection System (IPS), except that the purpose is to detect situations like distributed Denial of Service (DoS) attacks, while IPS is simply permitting or denying certain traffic.

Intrusion Prevention

When configuring IPS, the most important step is to catalog those data activities your network normally operates. Port 80 outbound from such-and-such server, 443 inbound and outbound, Network Basic Input/Output System (NetBios) and other Active Directory required protocols, File Transfer Protocol (FTP), and so on, each have legitimate purposes in most networks. The important point is to catalog the port, the expected origination, and the expected destination. Once that is documented, you can use that information to configure your IPS appropriately.

If you're configuring the network IPS, you'll need *all* the data relevant to that area of the network. If you're working on host IPS, you'll need expected transaction information for that host.

Integrity Monitoring

Tools like TripWire (www.tripwire.com) serve to monitor the Message Digest 5 (MD5) hash or checksum of the system files on your application or host. If alterations are made to these files, a good file integrity solution will detect and alert you to the issue.

To really make the best use of a configuration assurance tool, however, you will need to implement (assuming you have not already) a decent change management or configuration management database. You will also need solid processes around its use. An organization that is ISO-17799 compliant will typically have this sort of solution in hand already. Compliance can be a good thing! Solutions from NetIQ (www.netiq.com) can help in this area.

What are You Monitoring?

Focus your monitoring on the files that perform transactions or serve as libraries to your SOAP, XML, or ActiveX transaction applications. Alterations in these files serve as ingress points for additional misbehavior. The obvious point here is that if the file is altered, someone with ill intent is already accessing your network.

In addition, look into your OS' critical files. Monitor and alert on odd behaviors.

All the industry leading solutions in this space offer pre-configured solutions specific to varieties of software and operating systems. You should use these pre-configured packages to best protect your systems. However, applications that have been developed by small coding houses, or those you've written yourself, will need customization in order to be monitored. In this circumstance, your vendor must be willing to work with you to extend their technology to cover your gaps.

Again, if the vendor will not or cannot support your needs, take your business elsewhere!

Solutions Fast Track

Identity Management

- ☑ Develop and deploy a robust directory that is LDAP compatible.
- ☑ Design and deploy access control to each component of your PCI DSS environment.
- ☑ Certify that each component of your identity management solution can interface with those systems that provide you with identity data.
- ☑ Make certain each role for each user in your environment has a unique identifier that can be mapped back to a single identity (user).

Security Information Management

- ☑ Select a SIM vendor that can monitor all of the systems in your PCI DSS environment.
- ☑ Design a log aggregation solution that will scale to the eventual size of your environment.
- ☑ Deploy a storage solution that will handle the mass of data created by all the devices that generate logs.
- ☑ Identify each component of the PCI DSS environment. Where a component handles cardholder data or can facilitate access to cardholder data, you should be collecting logs from it.

Network and Application Penetration Testing

- ☑ Refer to PCI's list of ASVs and select one for ongoing penetration testing.
- ☑ Use a QSA to perform the actual assessment of your tools and processes.

Integrity Monitoring and Assurance

- ☑ Integrity monitoring solutions are necessary to make certain your core applications and host operating systems files are not altered. Tools from www.tripwire.com can help in this area.

☑ Configuration management solutions help you to understand your current operating environment, therein making it easier to configure the various solutions covered in this chapter. Tools from www.netiq.com can help in this regard.

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to **www.syngress.com/solutions** and click on the **"Ask the Author"** form.

Q: What is the difference between host intrusion detection and HIM?

A: Many different types of applications are labeled as host-based intrusion detection. In general, the distinction is that with a HIDS the end goal is the detection of malicious activity in a host environment, whereas a HIM system aims to provide visibility into all kinds of change. Detecting malicious change or activity is a big part of a HIM system, but that is not the entire motivation behind its deployment.

Q: My network IDS boats real-time processing of events. Should my HIM system be real time as well?

A: Not necessarily. There is a belief that real-time processing of host-based events is good because it is natural at the network level. This is simply not the case. Host-based integrity monitoring usually involves a great many more nodes compared with network monitoring. If you receive host-based alerts in real time, are you going to respond to them in real time? Usually the answer is no. The best way to stop attacks in their tracks is to prevent them from happening in the first place. The intrusion prevention product made by Immunix is a good example of this.

Q: I have a firewall. Do I need an IDS?

A: Yes. Firewalls perform limited packet inspection to determine access to and from your network. IDSes inspect the entire packet for malicious content and alert you to its presence.

Q: How many IDSes do I need?

A: The number of IDSes in an organization is determined by policy and budget. Network topologies differ greatly; security requirements vary accordingly. Public networks might require minimal security investment, whereas highly classified or sensitive networks might need more stringent controls.

Q: Do I need both HIDS and NIDS to be safe?

A: Although the use of both NIDS and HIDS can produce a comprehensive design, network topologies vary. Some networks require only a minimum investment in security, and others demand specialized security designs.

Q: Many of the statutes have overlapping control statements. Can I leverage output from a previous audit—say, PCI—to support SOX compliance?

A: To some extent, absolutely. Your auditor will determine to what extent, though. They can't totally rely on another auditors' work, but they can leverage some of it.

Q: I've gone through the PCI standard and it appears that the credit card companies want us to encrypt everything everywhere—for example, credit card numbers in repositories and even administrative connections to infrastructure devices. How can I achieve this, given my legacy environment?

A: The credit card companies realize that this is a challenge for many organizations. Because of this, they are relaxing PCI's encryption requirements. For specifics, contact your PCI auditor.

Q: When you are performing an external penetration test, should you worry about performing port scans too often?

A: In the last seven years or so, the Internet has become a very dangerous place for unprotected systems. Due to the proliferation of automated attack tools, port scans can fall into the background noise of a typical Internet-homed system. That being said, launching multiple scan threads from one source constantly will elevate your risk potential to someone watching the perimeter. An occasional scan may not be detected, but repeated ones might.

Chapter 10

How to Plan a Project to Meet Compliance

Solutions in this chapter:

- **Justifying a Business Case for Compliance**
- **Bringing all the Players to the Table**
- **Helping to Budget Time and Resources**
- **How to Inform/Train Staff on Issues**
- **Where to Start: The First Steps**

- ☑ **Summary**
- ☑ **Solutions Fast Track**
- ☑ **Frequently Asked Questions**

Introduction

You have determined that your organization needs to comply with the Payment Card Industry (PCI) Data Security Standard (DSS) and, looking at the requirements, you are not sure where to start. Should you jump in and go though the 12 PCI DSS requirements one at a time, ensuring that the requirements are in place, or should you first figure out at what level you need to comply. How will you make sure that your fellow associates are on board with the changes you are proposing so that you can comply with PCI DSS in an efficient manner? How will you make the compliance effort come together? After putting the plan together, how will you ensure that your fellow associates have the training and information in front of them to help keep your company from falling out of compliance? Putting together a comprehensive project plan will allow you to manage your compliance project efficiently and, in the end, achieve PCI DSS compliance.

This chapter will answer your questions about how to achieve compliance. You will learn how to justify putting in the effort and figure out if you need to comply at all. Once you know you have to comply with PCI DSS, we will help you bring all the players to the table to help build and enforce the compliance plan. We will give you tips on how to budget your time and resources so that you can achieve compliance quickly. Once you have your plan in place, you will need to get the message out to your staff and ensure they receive the right training to make sure your organization does not fall out of compliance. By the end of this chapter, you should have a clear plan on where to start with your own PCI DSS compliance efforts and the steps you will need to plan a project to meet compliance.

Justifying a Business Case for Compliance

One of the first steps of any compliance plan is to justify putting in the effort. You must first figure out if you need to comply with the PCI DSS regulation and also figure out if you have any overlap from other compliance plans that are already in place. Once you know compliance is a must, you need to figure out at what level you need to comply. PCI DSS compliance comes at four different levels and the requirements of compliance you need vary based on that level. The biggest question should be what is the cost of non-compliance. Compliance with the PCI DSS is mandatory. If you are not compliant you could be hit with fines and your credit card processing services could be terminated. That fact alone should help you justify putting in the effort.

Figuring Out If You Need to Comply

Your first step with any compliance effort should be figuring out if you need to comply with a regulation, so that you don't waste a lot of time putting in measures that you are not required to have. Once you have figured out what requirements you need to comply, it will help bring management and others on board to help you with the effort.

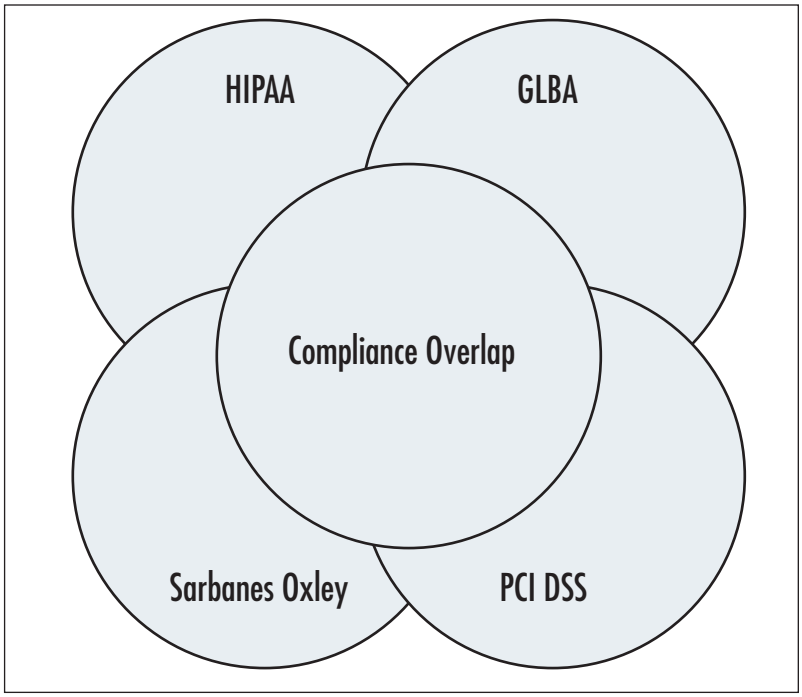
NOTE

To help your organization determine how many new policies and procedures you will have to put in place to become PCI DSS compliant, the Self-assessment Questionnaire should be completed in the early part of planning your compliance project. The Self-assessment Questionnaire is a good tool to help demonstrate what compliance you already have in place and will spell out what you need to do to become compliant. The self-assessment questionnaire can be downloaded from the PCI Security Standards Council Web site at www.pcisecuritystandards.org/tech/supporting_documents.htm.

Compliance Overlap

Once you determine that you have to comply, you need to look at what other compliance plans you have in place to see how you can leverage the investment you already made, which should help fast track your PCI DSS compliance plan. In the world of security regulations dealing with the protection of data, there is overlap (as shown in Figure 10.1) as most of the regulations are simply good business practices to have in place. So pull out your Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Sarbanes Oxley (SOX) compliance plans, and figure out which components you can reuse for your PCI DSS compliance plan. You might find that you are already in compliance, but need to document that the measures you have in place are consistent with the PCI DSS regulations.

Figure 10.1 Regulatory Compliance Overlap



Leveraging Compliance Overlap

To figure out how to leverage your other compliance efforts, the best place to start is to set up a meeting with the team leaders from that project. You need to get an idea of how the project went and how management accepted it. The main point is to find out what the other teams have done in their compliance effort and see what elements you can bring over into your PCI DSS compliance plan. For example, HIPAA and PCI DSS both have rules regarding encrypting data. Can you use your encryption policy and procedure from HIPAA for PCI DSS compliance? That answer will come as you talk to your HIPAA compliance team leaders and review the policy and procedure to see if it already fits the PCI DSS encryption requirement. Your company policy for HIPAA compliance should mandate that you have encryption in place as you transmit protected health information across public networks like the Internet. Requirement four of PCI DSS states that you need to encrypt cardholder data as it transmits across public networks. In this case, you do not need to recreate the wheel; you might just need to reclassify what type of data is required to be encrypted. Any efforts spent in leveraging your existing regulatory compliance will help to shorten the time it will take for you to become PCI DSS compliant.

The Level of Compliance

Now that you are on your way to planning your compliance project for PCI DSS, you need to figure out at which level you need to comply. Unlike other regulations that present you with an all or nothing stance on how to comply, PCI DSS compliance is based on how many credit card transactions a merchant processes. The more transactions that are processed the stricter the compliance plan will have to be.

For most organizations, compliance consists of passing a security network scan and completing a self-assessment questionnaire. If you process transactions in the millions, you will need to become certified as PCI DSS compliant by a certified vendor. To help you determine at what level your organization is at and what the compliance requirements are, see Table 10.1.

Table 10.1 PCI DSS Levels and Compliance Requirements

Level	Description	Compliance Requirements
1	Any merchant processing over 6,000,000 transactions per year. Any merchant that has been involved in a hack or attack that cased a data disclosure. Any merchant that PCI determines should be at level 1 to minimize risk to cardholder data.	Comply with DSS annual on-site security audit Quarterly network scans Validation by qualified security assessor and approved scanning vendor
2	Any merchant processing 1,000,000 to 6,000,000 Internet transactions per year.	Comply with DSS annual Self-assessment Questionnaire Quarterly network scans Validation by merchant and approved scanning vendor
3	Any merchant processing 20,000 to 1,000,000 Internet transactions per year.	Comply with DSS annual Self-assessment Questionnaire Quarterly network scans

Continued

Table 10.1 continued PCI DSS Levels and Compliance Requirements

Level	Description	Compliance Requirements
		Validation by merchant and approved scanning vendor
4	Any merchant processing fewer then 20,000 Internet transactions per year and all other merchants processing 1,000,000 transactions per year.	Comply with DSS Annual Self-assessment Questionnaire recommended Annual network scans recommended

What is the Cost for Non-compliance?

The question that should be answered during your justification process is what is the cost for not complying with PCI DSS. In all cases, the costs far outweigh the benefits of being compliant. Can your organization afford the fines and penalties, bad media press, and damage to its reputation?

In some cases when dealing with risk, you can look at what that risk is and deal with it in different ways. The options are whether to resolve the issue, transfer the risk, or ignore the risk. The way PCI DSS spells out its 12 requirements, the only way to truly deal with the elements are to resolve the issue or transfer the risk. Transferring the risk might mean that you outsource or bring in a managed service to deal with that requirement. Therefore, when you transfer the risk you are still dealing with it indirectly. Ignoring the risk in PCI DSS is not an option, because as you fill out your self-assessment questionnaire, if you answer no to any question, you are non-compliant. If you have a breach of data and auditors are brought in to verify your compliance, your penalties could be steep.

Penalties for Non-compliance

When your organization is found to be out of compliance with PCI DSS, the penalties can be severe. In some cases, the organization could be forbidden to store, process, or transmit credit card information. If you ran a retail store, think of the impact of not being able to process credit cards. This could cost you your business. Financial penalties and deeper audit requirements could also result. With the advent of new privacy laws in different states, you might be required to notify your customers of a

breach and also provide them with additional services such as credit reporting services. Once notifications go out, your organization's reputation could be dragged through the media. Looking at what it takes to comply, it should be easy to see how and why you need to put together your PCI DSS compliance plan.

Bringing All the Players to the Table

Once you have justified your compliance effort, it is vital that you bring all of the players to the table to ensure that a successful project will take place. You need the correct corporate sponsorship, otherwise senior management could reject any plan you put together. You need to look at your organization from the top down and identify each of the key people that are necessary to put the plan together, which will form your compliance team. You need to identify the key members of your team to tackle components of the compliance plan and keep the project moving.

Compliance plans can be won or lost based on the participants you bring in to help you with the project. It is vital to bring the correct people to the table as you need to be swift in putting your plan together. Look hard at the people you bring into your team, as they will either make putting together the compliance plan a success or a failure. Remember what non-compliance can bring; failure is not an option.

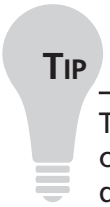
WARNING

Be sure to get a good understanding of the current workload of the members you would like to invite to be a part of your compliance team. Many times, people are enthusiastic to be a part of a new project, but realistically they do not have the time to work on it. What ends up happening is that team members miss meetings and/or deadlines, which will put a damper on your compliance project.

Obtaining Corporate Sponsorship

Management sponsorship is the critical success factor for any compliance effort. If senior management does not support the process, support from the staff will also lack. Why should they comply if your manager is not in compliance? As the leader of your compliance effort, you need to first work with your senior managers to help them become aware of the issues and let them understand the justification of why

you need to comply with PCI DSS. Make them understand the cost of non-compliance, and they will back you as soon as they realize that the company could be in jeopardy for not complying. Start at the top, because the sooner you gain support from the CEO, the faster you will get support from the Vice President and other senior management.



TIP

Try to schedule a lunch meeting outside of the office with the company CEO or other senior manager, where you would have his or her full attention, devoid of any distractions. Help him or her to understand the cost of non-compliance.

Attempt to get a senior manager on your compliance team. When other employees in the company hear that he or she is part of the team, the entire project will get more support, which will help drive home the fact that the compliance effort is vital for the organization.

Forming Your Compliance Team

Your compliance team is the focal point of your compliance project and is responsible for the success of the project plan. The best time to create your team is after you have received corporate sponsorship. Many times people who heard about the compliance project from a manager and want to participate will approach you. You need to get a good mix of people on the team to make the most impact. The PCI DSS has 12 requirements that can touch different departments in your company, so be sure to include at least one person from each of those functional areas. For example, PCI DSS requires you to build and maintain a secure network; therefore, if you do not get a team member involved from networking you cannot be sure that a firewall is installed or maintained going forward.

Roles and Responsibilities of Your Team

Your compliance team will help set the pace and scope of your compliance project. The selection of participants will make the project a success, but it is important to make it clear from the beginning which team member will be doing what by assigning roles and responsibilities to your team members. You will need your team to assist in the following ways:

- Work with managers and other team members to set the scope of the compliance project
- Select leaders for each of the areas where you need compliance
- Analyze information needed for the compliance plan
- Able to work with senior management to ensure that the end result is compliance

Getting Results Fast

The best way to ensure a successful project and gain the respect from all levels of your organization are to get results fast. As you are planning your compliance plan, you need to identify some low-level compliance issues and have your team tackle those first. People want to see results, and the faster you can show them results the more confidence they will have in the project. If it takes you months to get the first item addressed, people might wonder if the organization will ever be compliant and actually get complacent about the compliance effort as a whole. It could derail all of your efforts up to this point. Getting some results early on keeps the momentum and support moving in a positive direction for your entire project.

Notes from the Underground…

Bob's First Compliance Team

To give you a good example of how important it is to select the right team members, here is a real-world story of the first time "Bob" was on a compliance team.

I was approached by my manager to help with the compliance effort, as he felt that my knowledge would be an asset to the team. The team leader sent out a meeting request for the ten team members and I was excited to help make a difference in my organization. I showed up at the first meeting on time and ready to do what was necessary even if it meant having to put in overtime to get the job done. That first meeting did not go so well. The team leader was ten minutes late and only half of the team members showed up for the meeting.

Continued

Talking during the meeting, it was clear that none of the other senior managers were briefed on the compliance project and some even wondered if we needed to comply with these new laws. Senior management support wasn't there but the team leader knew we had to get in compliance or we would be in trouble. When I asked about the missing team members, the team leader thought that it was probably due to the lack of support from upper management.

After weeks of meetings, false starts, and many extra hours, we finally had senior management involved and then the wheels started to turn. The entire team showed up for a meeting for the first time, and we basically had to start over from the beginning. However, it was apparent that we did not have the right people for the team as the areas we were trying to become compliant in were not represented.

After a few more weeks, the right people did get involved with the team, and we still had senior management support. The project took off like a wild fire. We did a gap analysis and figured out what we needed to tackle and hit the ground running. After months of trying to put the team together, once we had the team in place we were able to knock out the entire project in three weeks. Just like the expression needing the right tool for the right job, you definitely need the right team for any compliance project you are attempting to pull off.

Helping to Budget Time and Resources

In order for your project to be a success you need to ensure that it is managed correctly and that it does not take too long to complete. As it was important for your team to get some results early on, you must continue to make sure that you set expectations, goals, and milestones. Figure out early on how you will manage the time and resources of your team and you will have a successful compliance project.

Setting Expectations

Setting expectations is a key factor when budgeting time and resources with your team. From the first stages of your compliance project, your team needs to know what to expect from you, other team members, and management. If this is a priority one project, the team needs to know that all other tasks are secondary until the compliance plan is in place. You also need to be sure you set the right expectations with management about what they should expect about the compliance plan.

Management's Expectations

Knowing from the beginning what management expects out of this effort should be one of your first tasks. Before you bring the team together, you should talk to senior management to make sure you understand what they expect out of the project and that you understand the timeline in which the project must be done. Also, be sure to understand the criticality of the compliance effort to the organization, as that will help you get a pulse on the project itself.

Once expectations of the compliance project are in place and management has signed off on these expectations, you need to document them and share them with all of the members of your team. By having all of the team members of the compliance project working with the same set of expectations, you are one step closer to having a successful project. If management feels the project needs to be done in four weeks but the team actually needs eight weeks to complete the tasks, be sure to set the correct expectations.

Establishing Goals and Milestones

Once a timeline is in place, it is important to set goals for the team on when key items should be complete. You want to make it very clear when project items are due and when parts of the compliance plan need to be in place.

Start by listing the goals of the project and assign those goals to team members. Make it clear when goals need to be met, as some will have prerequisites that must be finished before you can move on to the next task. Having goals in place will keep the project moving in the right direction. Set up milestones for success and publish your plan for everyone involved to keep up with what is complete.

A good way to keep your time and resources managed is by using project planning software such as Microsoft Project, which allows you to create Gantt charts that map resources to goals (see Figure 10.2). Gantt charts give you a way to easily report on your compliance project. If an item slips or is completed early, the chart will adjust and keep your project in line with the project timeline.

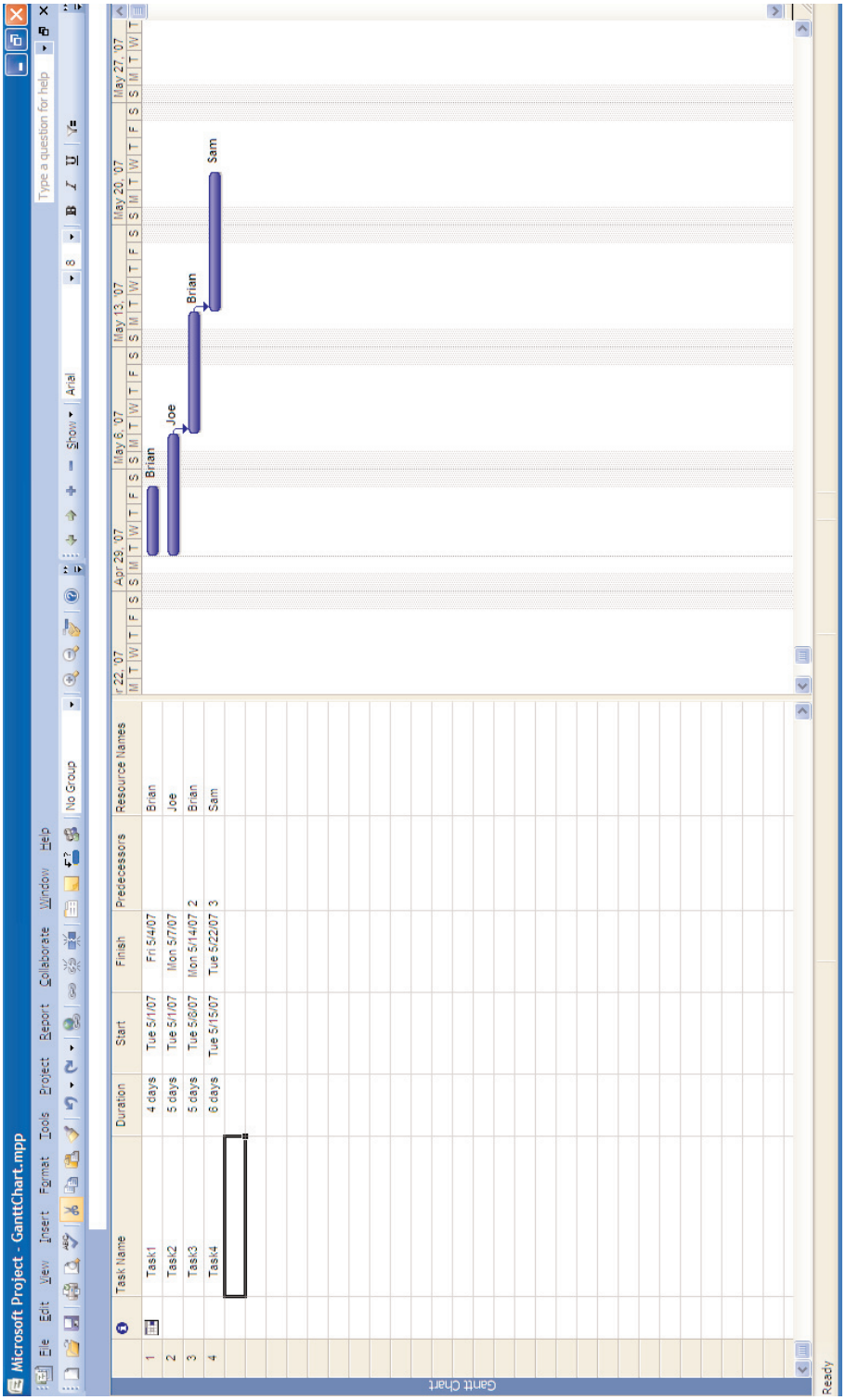


Figure 10.2 Example Gantt Chart

Having Status Meetings

The key to keeping your project on time is to have weekly team status meetings. The meetings should include your compliance team members and each should be prepared to report on what they have accomplished in the past week and what they will be working on in the next week. These meetings also give team members a chance to compare notes and bounce ideas off of each other if they are stuck on a problem.

You should also have status update meetings with the senior management team on a regular basis. Depending on the length of your project, the meetings should be, at a minimum, once a month. During these meetings you can go over your goals and milestones and show how the project is moving along. It will also give the senior managers a chance to give their input on the project and reinforce the support you need from them.

Be prepared to hand out copies of your working project plan Gantt chart. It will give a clear picture to your senior management team of where you are in the process and who is working on what issues. It is a good idea to send these charts to the managers beforehand to give them time to review the progress so that they can determine the guidance and support you will need.

How to Inform/Train Staff on Issues

Training can make or break any compliance project. You need to make sure from the first meeting that there is a training component to make sure all members know how the project will run and make sure they have all the necessary information to move forward with their part of the compliance project. Also, when your compliance program is in place, you need to make sure that part of that program includes training. Many of the PCI DSS requirements require that you maintain the requirement after it has been developed. The only way to do this is through a series of reminders and recurring training classes for your organization's employees. Having a training program in place from day one will go a long way in keeping your organization compliant after you have completed your compliance plan.

Training Your Compliance Team

When your compliance team meets for the first time you should divulge common information to all members. Items should include:

- An overview of the PCI DSS
- An overview of the PCI DSS compliance effort for your organization
- Why your organization is going through the process
- A review of the project plan itself at a high level to share goals and milestones
- A review of any elements the team might be submitting (i.e., how a policy should be written or status reports)

Training you compliance team will help to spell out how to accomplish putting the plan together and executing it to make your organization compliant. It will also get all members on the same page about what PCI DSS is and why your organization is going through the effort. You want to remove all myths around the project and level the playing field for your team members, so they can be successful in making your organization compliant.

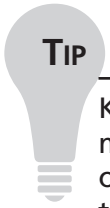
Training the Company on Compliance

After your project is complete and you deem your organization to be compliant, you need to make sure the rest of the company knows that you need to maintain a level of compliance. You do not want to have a violation in the first week because an employee did not know of the need for compliance.

You need to put together a corporate compliance training program that all new employees go through and that all employees go through annually, which acts as a refresher course and also gives you a chance to present any information that has changed over the past year.

Setting Up the Corporate Compliance Training Program

Be sure to set up your corporate compliance training program as an element of your compliance plan. Get the Human Resources department involved early on in the process, to make sure that all employees of your organization receive the training. Many times you can leverage existing programs (e.g., new employee orientation) by injecting your new hire training program into it.



TIP

Keep your compliance training program upbeat and fun. While security might be boring to most of your employees, it is fundamental to the success of your compliance efforts. One idea would be to have prizes at your training classes and offer them to people who get answers right during a question and answer session. People will be more likely to want to attend the training class if they can win a dinner, movies, or a gift card to any number of retail stores.

The compliance training program is more than just creating a one-time training class for your employees. The following elements should be incorporated for a successful program:

- Create a new hire training class that all new employees are required to attend. Work with your Human Resources department to see if this training class can be injected into an existing orientation program, or be sure you are a part of the process so your training team is notified about new hires.
- Create an intranet Web site that outlines key elements from the compliance training so employees have a good source to review information.
- Create a series of reminders to help keep the compliance effort on the minds of the employees. Good ideas for this are awareness posters, articles in your company's newsletter, and even compliance days where you can make a fun event around being PCI DSS compliant.
- Create a recurring annual training program for employees, to make sure they are reminded about what they need to do to comply. The recurring training program can work either as a live training class or a Web-based training class that they can take when time permits. Either way the training is presented, it should be required to keep your organization in compliance.

With the right training programs in place, you can be sure that from the first meeting of your compliance team to the annual recurring training for your associates, your compliance efforts will have a lasting effect on your organization.

Tools & Traps…

Posters as Reminders

One of the greatest tools in any compliance awareness program is the use of posters. With the use of posters you can get the message out quickly.

The posters you put out should have simple messages that grab people's attention. For PCI DSS compliance simple phrases such as, "Ensure your Anti-Virus is Up to Date" or "Keep all Cardholder Data Under Lock and Key" will get the message to your employees quickly.

Compliance posters are also a great way to get that first big result. You can create and put these posters up in the first part of your compliance planning efforts to give a kick start to the project. When senior managers are walking around the office, they will see the posters and see that you are taking the compliance project seriously.

Where to Start: The First Steps

It can seem like an overwhelming task to put together a compliance plan for PCI DSS. You are probably asking yourself where to start. Who do you get involved? When do you look at the PCI DSS Self-assessment Questionnaire? This section will get you pointed in the right direction and give you the first steps towards getting your organization compliant with PCI DSS.

The Steps

We know what we need to do to plan a project to meet compliance, but when it comes to PCI DSS what are the specifics you should be looking at to become compliant quickly and efficiently. (For an overview of the steps, see Figure 10.3.)

Step 1: Obtain Corporate Sponsorship

Once you have corporate sponsorship, you will have the backing for all of the steps of your compliance project plan. Be sure to meet with these members of your organization first to get the sign off and acceptance that your company needs to be PCI DSS compliant.

Remember, you need to make sure you get support from the highest level possible in your organization. Getting the backing from senior managers will help to ensure that the rest of the employees will be willing to work with you on getting compliant with PCI DSS.

Step 2: Identify and Establish Your Team

This is a critical step because it could make or break your compliance project. You need to be sure to select your team members from the appropriate areas of your company. Include the business leaders that have to worry about PCI DSS compliance and also the techies in the trenches who are setting up your networks. Having a good mix of key players will help your project succeed.

You should choose leaders for each of the 12 requirements of PCI DSS. If you break up each requirement you will be in a better position to complete your effort in a timely and concise manner. You should also set up a training class during your first team meeting to review what PCI DSS is, why your company has to comply, and the initial plan of what needs to be done to get into compliance.

Step 3: Determine your PCI Merchant Level

You need to know what your PCI merchant level is, which will tell you how you need to comply with PCI DSS. Talk with your team members that are from the business side, and figure out how many transactions you perform. Then refer to Table 10.2 to help you figure out your organization's PCI merchant level.

Table 10.2 PCI Merchant Levels

Level	Description
1	Any merchant processing over 6,000,000 transactions per year. Any merchant that has been involved in a hack or attack that cased a data disclosure. Any merchant that PCI determines should be at level 1 to minimize risk to cardholder data.
2	Any merchant processing 1,000,000 to 6,000,000 Internet transactions per year.
3	Any merchant processing 20,000 to 1,000,000 Internet transactions per year.
4	Any merchant processing fewer then 20,000 Internet transactions per year and all other merchants processing 1,000,000 transactions per year.

Knowing your merchant level will set the stage for what exactly you need to do to comply; each level has different requirements for compliance. It is important that you determine this early on in the process, because as you get closer to level one, your compliance effort will take longer and involve more resources. If you are not at level one from the start, you will want to periodically review how many transactions you are processing especially if you are on the border. If you slip to another level you will also slip out of compliance.

Step 4: Complete the PCI DSS Self-assessment Questionnaire

You need to complete the Self-assessment Questionnaire in one of your first compliance meetings, because the results of the questionnaire will give you clear guidance on how compliant your organization already is or is not with PCI DSS. The questionnaire can be found at the PCI Security Standards Council Web site at www.pcisecuritystandards.org/tech/supporting_documents.htm. If you answer "No" to any of the questions, you are not in compliance. The questions on the questionnaire map directly to the requirements of the PCI DSS. When your organization has the questionnaire complete, it will be indicate not only if you are compliant with PCI DSS, but what you need to do to become compliant.

Step 5: Get an External Network Scan from an Approved Scanning Vendor

Levels one though three require a network scan from an approved scanning vendor, and it is recommended at level 4. It is required that all externally exposed Internet Protocol (IP) addresses are scanned for vulnerabilities. It is also required that you use an external approved vendor, which means performing your own scans will not make you compliant. The PCI Security Standards Council maintains a list of approved scanning vendors at www.pcisecuritystandards.org/resources/approved_scanning_vendors.htm.

At the end of the network scan, the scanning vendor is required to provide you with a report that will show you if your Internet-facing network is PCI DSS compliant. If they discover a vulnerability, they will typically point you in the right direction toward a remedy.

WARNING

You must select your approved scanning vendor list that is maintained by the PCI Security Standards Council. If you do not use an approved vendor, any results you have, no matter how good they appear to you or your organization, can invalidate you PCI compliance efforts. Fines and penalties could result if you are found to be non-compliant.

Step 6: Get Validation from a Qualified Security Assessor

Currently, this step is only required if you determine that you are at merchant level one and requires that you bring in an external auditor onsite to review your PCI DSS compliance. You will want to engage the assessor to help you with Step 7 below, but ongoing, this is an annual process, where all components that are a part of how your company stores, processes, and transmits cardholder data is audited. You need to work with a qualified security assessor and a list of the QSA's, which can be found at https://www.pcisecuritystandards.org/resources/qualified_security_assessors.htm.

Step 7: Perform a Gap Analysis

After your team has gone through the questionnaire, the network scans the results and, if required, reports from your QSA prepare a document that lists out the gaps in your compliance effort. Your gap analysis document will set the stage for the creation of your compliance plan. To assist with your gap analysis, you should put together a worksheet that lists each requirement and indicates if you are compliant or not. You can also use the worksheet to initially assign the requirement to a compliance team member (see Table 10.3).

Table 10.3 PCI DSS Gap Analysis Worksheet

Requirement	Compliant (Yes/No)	Assigned To
Install and maintain a firewall configuration to protect cardholder data		
Do not use vendor-supplied defaults for system passwords and other security parameters		
Do not use vendor-supplied defaults for system passwords and other security parameters		

Continued

Table 10.3 continued PCI DSS Gap Analysis Worksheet

Requirement	Compliant (Yes/No)	Assigned To
Encrypt transmission of cardholder data across open, public networks		
Use and regularly update anti-virus software		
Develop and maintain secure systems and applications		
Restrict access to cardholder data by business need-to-know		
Assign a unique ID to each person with computer access		
Restrict physical access to cardholder data		
Track and monitor all access to network resources and cardholder data		
Regularly test security systems and processes		
Maintain a policy that addresses information security		

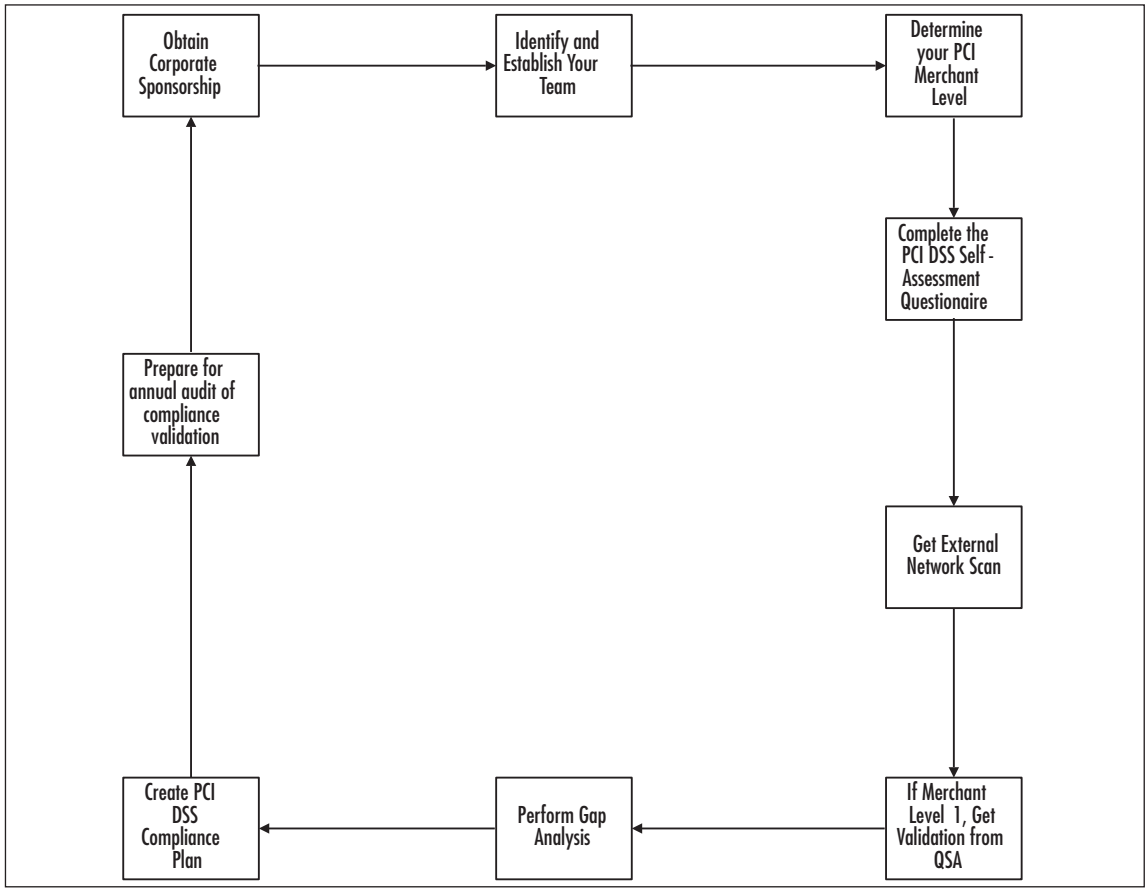
Step 8: Create PCI DSS Compliance Plan

Following the steps above, you now have the steps needed to create your PCI compliance plan. As we have discussed throughout this chapter, you should take all of these elements and bring them into your compliance plan. Your plan should include the gaps that are standing in the way of your PCI DSS compliance and what your organization plans to do to stay compliant year after year. Once all the gaps are closed, your compliance plan will be the live document that ensures you stay compliant and continue to maintain your organization's compliance to the PCI DSS.

Step 9: Prepare for Annual Audit of Compliance Validation

In order to maintain compliance, you should start over at step one and begin the process again every year. The good news is that most of what you need to do is already complete, and you are mainly validating and auditing the fact that you are still PCI DSS compliant.

Figure 10.3 Steps to PCI DSS Compliance



Summary

Planning a project to meet compliance can be so overwhelming that you could wind up having false starts or not begin the project at all. Your compliance efforts do not have to end this way. By putting together a good compliance project plan, you will have what it takes to make your organization PCI DSS compliant.

From the start of your project, you need to take a close look at why you need to become PCI DSS compliant. Simply figuring out if you need to comply can save you weeks of time. It is also critical that you determine what merchant level your organization is at. Based on the guidelines set forth by the PCI Security Standards Council, knowing your level will also help you justify what you need to do to be considered PCI DSS compliant. Again, if you spend the time and money to become level one compliant and you only need to comply at level four, you will have wasted time and money becoming level one compliant, which is much more time intensive and costly than becoming level four compliant. You also need to figure out what is the cost to your organization for non-compliance. Can your organization afford the risk? In all situations this answer should be no.

Once you determine that you need to be PCI compliant and cannot afford the risk of non-compliance, you need to bring all of the players to the table. You will first want to obtain corporate sponsorship and get the backing you need from senior management. The corporate sponsorship process will also help you form your compliance team. Your compliance project starts by getting your team together and beginning the planning process.

It is important that you guide your team in the right direction and help them budget their time and resources effectively. First, you need to set expectations with your team and management about what the compliance effort is all about. At this point, you can set up goals and milestones to help keep the project on a timeline and define when the project should be completed by. It is important to have status meetings with your team and with management during the process, to keep everyone informed and moving forward on the project.

As you start your compliance planning project, make sure that your team members get the correct training by providing an overview of what PCI DSS is and why your organization is going though this compliance effort. You should also train all of the employees in your company in what it takes to be and stay compliant. Setting up a corporate compliance training program will have a lasting effect on your organization, not only in keeping PCI compliant, but also keeping your workforce thinking about security at all times.

We also outlined the nine steps you should take to become PCI DSS compliant. If you go through each of these steps you will have a completed compliance effort. Knowing that you are PCI compliant will help to get rid of the fears of non-compliance by management, which in turn will help make your organization more successful.

At the end of your compliance effort, congratulate the team and encourage them to continue to help keep your organization PCI DSS compliant for as long as your company stores, processes, and transmits cardholder data.

Solutions Fast Track

How to Justify the Effort

- ☑ Make sure that you are required to comply, otherwise, you might be more secure as an organization but probably wasted a lot of time putting in measure that you were not required to do.
- ☑ Figure out what is the level of compliance your organization will have to comply at, to be sure you have all the necessary compliance requirements in place.
- ☑ Figure out what is the cost of non-compliance and whether or not your organization can justify taking on that risk.

Bringing all the Players to the Table

- ☑ First gain corporate sponsorship within your organization as your senior managers will provide you with the necessary support to get your company into compliance.
- ☑ Your compliance team will help set the pace and scope of your compliance project; therefore, the selection of the participants is vital to the success of the project.
- ☑ As you are planning your compliance plan, identify what to tackle first to get results quickly, by showing your team what it takes to get your organization compliant with PCI DSS.

Helping to Budget Time and Resources

- ☑ From the first stages of your compliance project your team and management needs to know what to expect of the compliance effort.
- ☑ Establish goals and milestones to keep your team and management on track with the compliance planning processes.
- ☑ Have status meetings with both your team and management to keep everyone moving forward on the path of compliance. These meetings will help show the progress of what has been accomplished and what is left to accomplish.

How to Inform/Train Staff on Issues

- ☑ Compliance team training will get all members on the same page about what PCI DSS compliance actually is, and why your organization is going though the effort of compliance.
- ☑ Set up a corporate compliance training program to make sure your employees understand what it takes to be PCI DSS compliant and stay compliant on an ongoing basis.
- ☑ Create a recurring annual training program for employees, to make sure they are reminded about what they need to do to keep the organization compliant.

Where to Start: The First Steps

- ☑ Step one in your compliance planning should be obtaining corporate sponsorship, which will give you the backing you need for the compliance effort.
- ☑ Depending on the merchant level you are at, perform an external network scan and/or get validation from a qualified security assessor.
- ☑ Perform a gap analysis early on in your process to determine where you are already in compliance and where you need to do work to get in compliance.

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to **www.syngress.com/solutions** and click on the **"Ask the Author"** form.

Q: What should be your first step with any compliance effort?

A: Figuring out if you even need to comply.

Q: How should you deal with compliance overlap?

A: Use any other past compliance efforts your company has been through to kick start your PCI DSS compliance effort. You might find that while getting in compliance with SOX you are already in compliance with PCI DSS.

Q: How many merchant levels does the PCI DSS have?

A: Four.

Q: What defines a level one merchant?

A: Any merchant processing over 6,000,000 transactions per year and/or involved in a hack or attack that caused a data disclosure.

Q: What could be the one penalty for non-compliance of the PCI DSS that could put a company out of business?

A: Your organization could be forbidden to store, process, or transmit credit card information.

Q: If senior management does not support the compliance planning process, what can you expect?

A: You can expect the support from the rest of the staff to be in line with senior management.

Q: Why is it important to clearly define the roles and responsibilities of your compliance team members?

A: Your compliance team will set the pace and scope of your compliance project. Selecting the right people from the right functional areas of your organization will make it possible to get your company in compliance.

Q: Why are getting results fast important to your team?

A: Getting some results early on keeps the momentum and support in a positive direction for your entire project.

Q: Why is it important to understand senior management's expectations?

A: You need to understand the criticality of the compliance effort for the organization, which will help drive the project itself. Knowing the expectations of senior management will lead to a successful project plan.

Q: What is a good way to keep your time and resources managed?

A: Use a project planning tool that allows you to create Gantt charts, which will map resources to goals over time.

Q: What is the importance of status meetings with your compliance team?

A: The status meetings will help keep your project running on-time, and give members a chance to compare notes with other team members and throw ideas off each other if they are stuck with a problem.

Q: What is one factor of the importance of training your compliance team?

A: It will help to remove all myths around the project, and level the playing field for your team members so they can be successful in making your organization compliant.

Q: Which department in your corporation should be involved in the training program for your entire company?

A: Human Resources should be involved in the corporate compliance training program, as many times you can leverage existing programs that are already in place, such as new employee orientation.

Q: What is the importance of recurring training for the employees of your organization for any compliance effort?

A: Recurring annual training will make sure that your employees are reminded about what they need to do to continue to comply with your company's policies and procedures.

Q: What is the importance of the PCI DSS Self-assessment Questionnaire?

A: The results of the questionnaire will give you clear guidance on how compliant your organization already is with the PCI DSS.

Q: What is a gap analysis?

A: The gap analysis is the process in which you take your results from the Self-assessment Questionnaire, the network scan results, and, if required, any reports from the qualified security assessor, and determine the areas in which you need to shore up to become PCI DSS compliant.

Q: What is required by the external network scan by an approved scanning vendor?

A: It is required that all externally exposed IP addresses are scanned for vulnerabilities and are corrected if any vulnerability is found.

Chapter 11

Responsibilities

Solutions in this chapter:

- **Whose Responsibility is it?**
- **Incident Response**
- **Forensics**
- **Notifications**
- **Liabilities**
- **Business Continuity**
- **Disaster Recovery**

- ☑ **Summary**
- ☑ **Solutions Fast Track**
- ☑ **Frequently Asked Questions**

Introduction

Everyone who is a stakeholder has the responsibility of ensuring Payment Card Industry (PCI) data is protected from unwanted disclosure, modification, or destruction of data in a system, from the end user, to the retailer, to the credit card company. But moreover, when an incident occurs, the organization that is storing the PCI data is the one held accountable. Upper management is held accountable for the security of PCI data. Most of us are familiar with the types of incidents that can occur on a daily basis. These include but are not limited to:

- The vulnerabilities or misconfigurations that might lead to a system compromise affecting the overall confidentiality, integrity and availability of the system and data.
- The viruses, worms, Trojan horse programs, keystroke loggers, rootkits, logic bombs, spam relays, and remote control bots that can degrade system resources and capture confidential data.
- The detection or discovery of unauthorized users or users with elevated privileges in excess of what is required to perform a specific duty (principle of least privilege).
- The loss of computing devices.

There are certain steps that must be taken when one of the before mentioned events does occur that will your organization get back to normal quicker. In this chapter we'll briefly discuss whose responsibility it is to protect PCI data, Incident Response Teams (IRT), forensics, notifications, liabilities and business continuity, and disaster recovery.

Whose Responsibility Is It?

A good security policy sets the stage for the entire organization and establishes responsibilities for all the employees, from the Chief Executive Officer (CEO) down to the end user. Requirement 12 of the PCI DSS v1.1 establishes the requirement of a policy that addresses information security for employees and contractors. Of all the users in an organization, probably the most important position within an organization's security policy is the CEO.

CEO

The CEO must support the security policy and ensure that everyone else understands his or her responsibilities as well. Without formal buy-in and support of the security policy, the policy will not be worth much more than the paper it's printed on. Besides, when a severe incident occurs, and your organization ends up on the front page of the daily newspaper, the CEO is the one who gets to speak with shareholders and the public and hopefully keep the organization in good standing. So in addition to running the organization, the CEO must also:

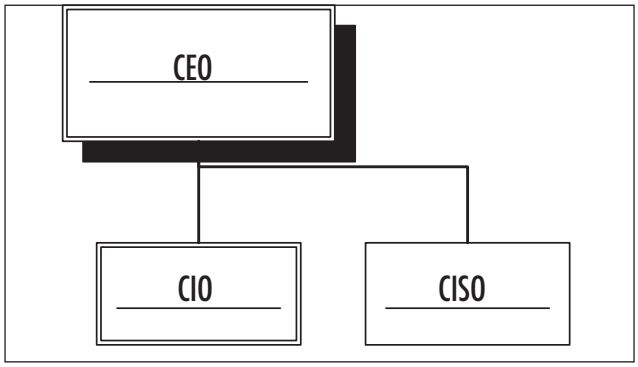
- Ensure that information security is taken into consideration in all systems being developed or acquired by the organization.
- Provide vulnerability mitigation and an incident response capability.
- Ensure that all contracts with third-party vendors or partners include provisions to protect PCI data at their sites as well.
- Ensure the appropriate notice of privacy rights and security responsibilities are provided to all personnel accessing his organization's systems.
- Ensure that sound information security practices are being implemented on all systems.
- Provide annual security awareness training to all staff.

This sounds like a lot of work for the top position in a company. It's a full time job. But in most cases the first thing a CEO will do is appoint a Chief Information Security Officer (CISO) to ensure that all information security functions are being performed as stated in the organization's security policy. It's just not practical to expect the CEO to be able to ensure that all information security-related functions are performed.

CISO

The CISO or Chief Security Officer (CSO) is responsible for the security control mechanisms of information technology within the organization. The CISO, in most cases, will report directly to the CEO on all security-related issues, as shown in Figure11.1.

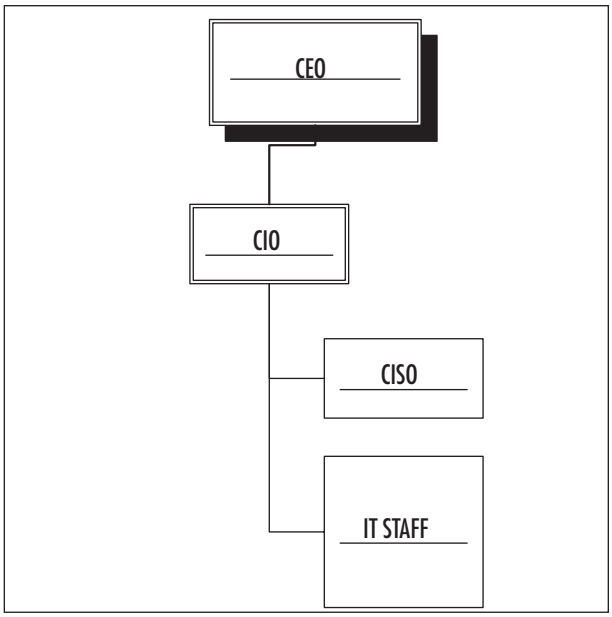
Figure 11.1 Direct Reporting



There is some debate here. Some organizations have the CISO report directly to the CEO so the CEO has an unbiased view of the state of security in the organization (a watchdog). Many organizations have the CISO report through the Chief Financial Officer (CFO). See this article from www.CSOonline.com in February of this year: http://blogs.csoonline.com/ciso_trends_gaining_power_or_losing_positions.

Others choose to put the CISO under the CIO, since the CIO is appointed as the overall responsible person for information systems in the organization, thus making the CISO report any security related issues to the CIO as in Figure 11.2.

Figure 11.2 CIO Reporting



From a high level, the CISO role focuses on the information and physical security strategy within an organization. This security strategy varies depending on the needs of your organization, but often includes, at a minimum, responsibility for the following items:

- Security Office Mission and Mandate Development
- Security Office Governance
- Security Policy Development and Management
- Security Training and Awareness Development
- Security Project Portfolio Development

To get a little more granular, the CISO's duties should include but are not limited to the following:

Network Monitoring Responsibilities:

- Manage and maintain a current inventory of Information Technology (IT)-related inventory to include topologies detailing the approximate location of all computer hardware and software owned by the organization.
- Review daily/weekly reports generated by firewalls and intrusion detection solutions.
- Review daily/weekly server and application event logs and user activity reports.
- Review all external audit reports related to IT.
- Review assigned access rights for network access and core applications of all users in the organization, to ensure that the proper privileges are assigned.
- Review weekly Antivirus Application reports to ensure that application is performing correctly and updates are being received.
- Monitor and ensure all password files are protected and closely monitored for compromise.

Support and Implementation Responsibilities:

- Ensure the proper implementation of the Information Systems Security Policies and Procedures.
- Provide consultation and assistance to employees and management within the organization regarding security procedures.
- Ensure all employees understand and acknowledge the Desktop and Terminal Guidelines and are familiar with the organization's IRP.
- Review security-related procedures of the BCP/Disaster Recovery Policies for effectiveness.
- Monitor new potential threats and keep the organization informed of such threats.
- Report to the CEO on all security-related deficiencies discovered along with recommendations for corrective actions.
- Consult with the CEO regarding recommendations on security procedures.
- Review and recommend changes to policies as needed to the CEO.
- Maintain control over the issuing of access rights and permissions for all critical applications within the organization, thereby ensuring access requests are consistent with the security policy.
- Provide annual security awareness training to all employees.

The CISO also has a staff to work with. These staff members are usually charged with auditing systems for compliance such as ensuring patches are up-to-date, virus definitions are current, user accounts are deleted when no longer needed, logging is enabled, and specific security features have been put in place to secure a system or application.

NOTE

The CISO focuses on the information security of the entire organization and uses the security policy and the backing of the CEO to ensure security. Compliance and governance are key functions for the CISO. The responsibilities can be very detailed or left at a higher level to leverage changes to the security policies and procedures.

CIO

The CIO is the head of the IT group within an organization. The CIO usually reports to the CEO. The CIO is a key contributor in formulating strategic goals for an organization. So, you can see where there might be some friction in an organization where the CISO reports directly to the CEO vs. the CIO. The CIO should know if there are security issues on his or her systems. Having the CISO report directly to the CEO sometimes emanates to the organization that IT cannot be trusted to secure their systems. The prominence of this position has risen greatly as information technology has become a more important part of business. The CIO may be a member of the "executive board" of the organization, but this is dependent on the type of organization.

Security and System Administrators

Your Security and System Administrators (SECAdmins) have the responsibility of actually implementing the security policy for the organization. For the System Administrators (SAs) this is simple. The SA's primary responsibility is the maintenance of the systems and ensures up time. So, as for implementing security features, the SA should only implement security features that are recommended and approved by management.

SECAdmins are responsible for all security aspects of a system on a day-to-day basis, whether it is a network appliance or a database system. The SECAdmin should be independent from development and operations staff. The SECAdmin is often the most trusted resource in an organization, and may have privileged access in order to access the most sensitive information and activities. The SECAdmin helps to develop sound rule sets for the firewalls and intrusion detection systems (IDSes). The SECAdmin may also have the responsibility of implementing, with the SA's assistance, specific security features on individual systems. Additionally, the SECAdmin will probably have the responsibility of ensuring log files are being produced, archived, and audited and any findings reported back to the CISO.

Additional Resources

The responsibility of security doesn't stop with the CEO, CIO, CISO, SECAdmin, and SAs. Security should be embraced throughout the organization. Each of the other departments within your organization has the responsibility of adhering to the security policy and ensuring that PCI data is not compromised. Moreover, each

individual should know what to do in the event data does become compromised or there is a security incident.

Incident Response

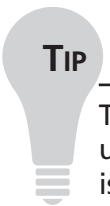
The purpose of incident response (IR) plans and procedures is to provide a systematic approach as well as a general guideline for your organization's staff on procedures to be followed whenever abnormal or unusual situations occur, which may affect daily operations and ultimately compromise PCI data. Another purpose for incident response procedures existence is ensuring business continuity in a timely but organized manner to include documenting the event in a manner so that management can analyze procedures undertaken and address short comings if the event occurs again in the future. We'll discuss business continuity and disaster recovery later in this chapter. Therefore, IR should address procedures that assist the staff to:

Respond to incidents systematically.

- Help personnel to recover quickly and efficiently from incidents, minimizing the loss or theft of information and service disruptions.
- Using information gained during incident handling to better prepare for handling future incidents.

Deal properly with legal and media issues that often arise during and after an incident.

I don't really think I could get through this chapter without pointing out the Visa USA Cardholder Information Security Program (CISP). CISP provides the tools and measurements needed to protect against cardholder data compromise. They even have specific guidelines on what to do in the event of a compromise. But even so, every organization needs to have a good Incident Response Program (IRP). The IRP starts with the formation of an IR Team.



TIP

The CISP provides a good document on what to do if compromised at http://usa.visa.com/download/merchants/cisp_what_to_do_if_compromised.pdf. This is a good resource when planning for or responding to an incident.

Incident Response Team

Again, the IRT is another area that needs management and constituency buy-in for the vision and mission of the IRT. Once the creation of an IRT is granted you must:

Appoint and train the IRT staff.

- Procure equipment and provide the infrastructure to support the team's mission.
- Develop the policies and procedures to support IRT services.
- Define the specifications for and build your incident-tracking system.
- Develop incident-reporting guidelines for your organization and clientele. Incident reporting procedures include as much detail as possible to alleviate confusion. They should include what medium can be used for submitting reports (e.g., e-mail, pager, phone, Web forms, and so on). It should also include details about what type of information should be included in the report.
- Develop a process for responding to incidents. This includes how the IRT will prioritize and respond to received reports, response timeframes, and notifications. Also, an after-action report should be created to discuss lessons learned and to provide closure to the original party reporting the incident.

Now that an IRT has been formed, what exactly are they supposed to do? They execute the IRP. Should an IRP come before the IRT? It's open to debate. In my experience there is usually a requirement to have an IRP in place. This drives the need to create the IRT to execute it.

Incident Response Plan

It is important that IRPs are supported throughout the organization, and tested regularly. A good incident response plan cannot only minimize the affects of a security incident, but can also reduce any negative publicity that often follows. There is something to be said about the positive aspect of knowing that a security incident will occur. It allows your IRT to develop the appropriate course of action to minimize damages. Combining this course of action with subject matter expertise allows the IRT to respond to incidents in a systematic and formal manner.

The IRP should be clear and concise and executed quickly. When an IRP is executed, there is little room for error. For this reason, the IRP should be practiced regularly and scenarios staged to provide as much exposure to the procedures to the staff on specific incidents. Testing makes it possible for methodologies to be developed that allow for timeliness and accuracy, minimizing the impact and damages in the event of an actual compromise. An IRP has a number of requirements, to include, but not limited to:

- The creation of an IRT to execute the plan.
- Legal approval
- An appropriate budget
- Upper management buy-in/support
- An action plan
- Appropriate resources (i.e., standby systems (hot, cold), backup devices/services, redundant storage)

Forensics

If you have determined your PCI data or system has been compromised, as a Visa member, you must seek the professional help of a Qualified Incident Response Company (QIRC) to perform a forensic investigation. Forensics is more than just an impromptu investigation. The term forensic pertains to the art or study of argumentation to be used in a court of law or public discussion and debate.

WARNING

When performing any investigation, the federal rules of evidence should be followed to ensure it is allowed in the court of law in the event legal action is required. Details concerning these rules can be found at www.uscourts.gov/rules/ and additional information can be at www.usdoj.gov/criminal/cybercrime/s&smanual2002.html.

There are specific guidelines that must be followed. The following actions are included as part of the forensic investigation:

1. Determine cardholder information at risk:

- Card type
- Information at risk
- Cardholder name, address, account number, expiration date
- Personal Identification Number (PIN) blocks
- Magnetic strip data
- Timeframe of the compromise

In essence, all the data that was possibly compromised needs to be gathered.

2. Perform incident validation and assessment:
   - Determine the timeframe of compromise.
   - Determine how the compromise occurred.
   - Identify the source of the compromise (i.e., network, system, Web site, developmental systems, end user, VPN, modem, and so on).
   - Determine if the compromise has been contained. Containment is critical. You cannot correct the problem without first containing the incident to a specific area.
3. Check for Track 1 and Track 2 data, Card Verification Value (CVV2), and/or PIN block storage, whether encrypted or unencrypted. Identify all locations where this data may reside.
4. Identify the vendor name, product name, and version number if track data, CVV2, and/or PIN blocks are stored by a payment application,
5. If applicable, review VisaNet endpoint security and determine the risk.
6. Preserve all potential electronic evidence on a platform suitable for review and forensic analysis by a court of law if needed.
7. Perform an external and internal vulnerability scan.

NOTE

At any time Visa reserves the right to engage their incident response team without regard to the size or complexity of the incident.

By using proper forensic techniques you will avoid costly discovery motion practices and allow you to gather and preserve the right data at the right time using early computer discovery planning tools. You will also avoid the traps of improperly mishandling, identifying, and preserving computer data.

Notification

Your IRP should include procedures on notification to the rest of the organization, Visa, your customers, law enforcement, and possibly the media. The Visa U.S.A. Inc. Operating Regulations, the Plus System Operating Regulations, and the Interlink Network Operating Regulations, require that members comply with the Visa USA Cardholder Information Security Program (CISP) by immediately reporting a security incident and the suspected or confirmed loss or theft of any material or records that contain cardholder data.

Your organization may need to communicate with outside parties regarding an incident. This includes reporting incidents to organizations such as the Federal Computer Incident Response Center and law enforcement, and also fielding inquiries from the media. One reason that many security-related incidents do not result in convictions is that organizations do not properly contact law enforcement. Several levels of law enforcement are available to investigate incidents:

- The Federal Bureau of Investigation [FBI]
- The U.S. Secret Service
- District Attorney Office
- State Law Enforcement
- Local (e.g., county) law enforcement

Law enforcement should be contacted through designated individuals in a manner consistent with these procedures. The spokesperson will be familiar with the reporting procedures for all relevant law enforcement agencies and well prepared to recommend which agency, if any, should be contacted.

Customer notice should be provided whenever it becomes aware of an incident of unauthorized access to customer information and, at the conclusion of a reasonable investigation, determines that misuse of the information has occurred or it is reasonably possible that misuse will occur. Customer notice should be given in a clear and conspicuous manner. The notice should include the following items:

- Description of the incident
- Type of information subject to unauthorized access
- Measures taken by the institution to protect customers from further unauthorized access
- Telephone number customers can call for information and assistance
- Remind customers to remain vigilant over next 12 to 24 four months, and report suspected identity theft incidents to the institution

Additionally, customer notice should be delivered in a manner designed to ensure that a customer can reasonably be expected to receive it. For example, the institution may choose to contact all customers affected by telephone or by mail, or by electronic mail for those customers for whom it has a valid e-mail address and who have agreed to receive communications electronically.

Liabilities

So, what happens if your data is compromised? You'd probably expect that credit card companies would hold the source of the compromise financially liable, especially if a retailer was storing card data in violation of the PCI DSS. But are retailers really being held to that standard? What are the consequences of non-compliance? Anyone who works with PCI data should already know what the fines are like. The penalties for non-compliance are severe. The Visa Web site states that Visa members are subject to a penalty of $100,000 per incident if the member fails to immediately notify Visa USA Fraud Control of the suspected or confirmed loss or theft of any Visa transaction information. Visa members can also be fined up to $500,000 per incident, if it is determined that the service provider is not compliant at the time of the incident. Further information can be found at http://usa.visa.com/merchants/risk_management/cisp_if_compromised.html. These are pretty stiff fines, but that's only the beginning.

Besides the fines that can be induced by Visa, your organization has to bear the brunt of any lawsuits from customers that may stem from the incident. This could be in the hundreds of thousands of dollars as well. So, there is a possibility of several hundred thousand dollars in fines depending on the severity and the timeliness of the notification. But that's not all. Once the media gets a hold of the information, the loss of trust by the customer and client base can be deadly. If customers and clients terminate their relationships with the vendor, it could actually put you out of business depending on the severity of the incident.

Business Continuity

Disaster recovery is the process by which an organization resumes normal operations after a disruptive event. The event might be something huge like a hurricane or something less catastrophic, but equally as severe in terms of potential data loss, like a failed server caused by a computer virus. Business continuity is also the process by which an organization resumes normal operations, but at an alternate site for a prolonged period of time. The two terms are often combined in an organization under the acronym BC/DR. At any rate, BC/DR determines how a company will keep functioning after a disruptive event until its normal facilities are restored.

As a consumer, we demand our information remain private and stay safe. As a credit card vendor, we have to ensure that PCI data remains private and stays safe. BC/DR planning is essential for the continuation of services to your customers in the event of an unexpected occurrence, which seriously disrupts the business process. The documentation under BC/DR, established by your organization, is to ensure that it is operating under its established guidelines for safety and soundness as well as the protection of confidential data. We will focus on the confidential data part, PCI data. What does it do for you? A sound BC/DR plan provides the ability to respond to a variety of potential disasters faster based on available resources and the relative likelihood of occurrence. There is also cost savings realized by being efficient through the use of time and money.

BC/DR planning is about maintaining, resuming, and recovering the business, not just the recovery of the technology. Creating and deploying a plan that identifies the infrastructure and processes required to provide an acceptable level of service if a critical business process fails due to the sudden loss or degradation of a system(s) or possibly even the failure of an outsourced system or service. This plan should be initiated, reviewed, and tested periodically to ensure that the process works.

Summary

Securing PCI is everyone's responsibility in the organization. The CEO may be ultimately responsible, but he also knows to hire the right people to do the job. That CISO is hired to perform the tasks and assume the responsibility of maintaining the information security for the entire organization. In many cases, the CISO reports directly to the CEO to provide an unbiased view of the state of security in an organization. Other organizations may choose to have the CISO report to the CIO, since the CIO has the overall responsibility for all information systems and networks within the organization.

IR procedures are put in place to respond to incidents systematically, and to recover quickly and efficiently for incidents, minimizing the loss or theft of information or service disruptions. The information gathered during an incident is used to better prepare the IRT for future incidents of the same nature. IR procedures also help to properly deal with legal and media issues during and after an incident. The IRT is critical in making sure that your organization's IRP is executed properly.

Forensics can be very tricky. As a Visa member, you must seek the professional help of a Qualified Incident Response Company (QIRC) to perform a forensic investigation. Remember, forensics pertains to the area or study of argumentation to be used in a court of law. Always try to follow the rules of evidence to ensure it is allowed in court in the event legal action must be taken. Visa reserves the right to engage their IRT at any time once an incident has been reported. More information on IR and forensics can be found in the CISP.

Remember, once an incident occurs, notification needs to be sent out to Visa, your customers, law enforcement, and possibly the media. Law enforcement should be contacted through designated individuals in a manner consistent with reporting procedures. Customer notice should be provided whenever it becomes aware of an incident of unauthorized access to customer information and, at the conclusion of a reasonable investigation, determines that misuse of the information has occurred or it is reasonably possible that misuse will occur. Additionally, customer notice should be delivered in a manner designed to ensure that a customer can reasonably be expected to receive it.

The penalties for non-compliance are severe. The Visa Web site states that Visa members are subject to a penalty of $100,000 per incident if the member fails to immediately notify Visa USA Fraud Control of the suspected or confirmed loss or theft of any Visa transaction information, Visa members can also be fined up to

$500,000 per incident, if it is determined that the service provider is not compliant at the time of the incident. Besides the fines that can be induced by Visa, your organization has to bare the brunt of any lawsuits from customers that may stem from the incident. You may also lose your customer base depending on the severity of the incident.

Disaster recovery is the process by which an organization resumes normal operations after a disruptive event. Business continuity is also the process by which an organization resumes normal operations, but possibly at an alternate site for a prolonged period of time. The BC/DR is essential for the continuation of services to your customers in the event of an unexpected occurrence, which seriously disrupts the business process. The documentation under BC/DR, established by your organization, is to ensure that it is operating under its established guidelines for safety and soundness as well as the protection of confidential data. BC/DR planning is about maintaining, resuming, and recovering the business, not just the recovery of the technology. Creating and deploying a plan that identifies the infrastructure and processes required to provide an acceptable level of service if a critical business process fails due to the sudden loss or degradation of a system(s), or possibly even the failure of an outsourced system or service.

Whose Responsibility Is It?

- ☑ Without formal buy-in and support of the security policy, the policy will not be worth much more that the paper it's printed on.
- ☑ The CISO is responsible for the overall security control mechanisms of information technology within the organization.
- ☑ This security strategy varies depending on the needs of your organization, but often includes responsibility for the following items: Security Office Mission and Mandate Development, Security Office Governance, Security Policy Development and Management, Security Training and Awareness Development, Security Project Portfolio Development.
- ☑ The CISO focuses on the information security of the entire organization, and uses the security policy and the backing of the CEO to ensure security.
- ☑ The SA should only implement security features that are recommended and approved by management.

Incident Response

- ☑ The purpose of incident response plans and procedures is to provide a systematic approach as well as general guideline for your organization's staff on procedures to be followed whenever abnormal or unusual situations occur.
- ☑ CISP provides the tools and measurements needed to protect against cardholder data compromise.
- ☑ It is important that IRPs are supported throughout the organization.
- ☑ The IRP should be clear and concise and executed quickly.
- ☑ Testing makes it possible for methodologies to be developed that allow for timeliness and accuracy, minimizing the impact and damages in the event of an actual compromise.

Forensics

- ☑ As a Visa member, you must seek the professional help of a QIRC to perform a forensic investigation.
- ☑ When performing any investigation, the federal rules of evidence should be followed to ensure it is allowed in the court of law in the event legal action is required.
- ☑ At any time, Visa reserves the right to engage their incident response team without regard to the size or complexity of the incident.
- ☑ By using proper forensic techniques, you will avoid costly discovery motion practices and allow you to gather and preserve the right data at the right time using early computer discovery planning tools.

Notification

- ☑ The Visa U.S.A. Inc. Operating Regulations, the Plus System Operating Regulations, and the Interlink Network Operating Regulations, require that members comply with the Visa USA CISP by immediately reporting a security breach and the suspected or confirmed loss or theft of any material or records that contain cardholder data.

- ☑ Law enforcement should be contacted through designated individuals in a manner consistent with these procedures.
- ☑ Customer notice should be provided whenever it becomes aware of an incident of unauthorized access to customer information and, at the conclusion of a reasonable investigation, determines that misuse of the information has occurred or it is reasonably possible that misuse will occur.

Liabilities

- ☑ Visa members are subject to a penalty of $100,000 per incident if the member fails to immediately notify Visa USA Fraud Control of the suspected or confirmed loss or theft of any Visa transaction information,
- ☑ Visa members can also be fined up to $500,000 per incident if it is determined that the service provider is not compliant at the time of the incident.

Business Continuity

- ☑ Disaster recovery is the process by which an organization resumes normal operations after a disruptive event.
- ☑ BC/DR determines how a company will keep functioning after a disruptive event until its normal facilities are restored.
- ☑ The BC/DR is essential for the continuation of services to our customers in the event of an unexpected occurrence, which seriously disrupts the business process.
- ☑ A sound BC/DR plan provides the ability to respond to a variety of potential disasters faster based on available resources and the relative likelihood of occurrence.
- ☑ BC/DR planning is about maintaining, resuming, and recovering the business, not just the recovery of the technology.

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to **www.syngress.com/solutions** and click on the **"Ask the Author"** form.

Q: Who is ultimately held accountable if PCI data is compromised in an organization?

A: The CEO is the top position in the organization and is ultimately responsible for the security of PCI data.

Q: What requirement of the PCI DSS v1.1 establishes the requirement of a policy that addresses information security for employees and contractors?

A: Requirement 12.

Q: What position is appointed to champion the security efforts within an organization and either reports directly to the CEO or the CIO?

A: The CISO is responsible for ensuring the security policy is implemented throughout the organization.

Q: A security strategy often includes what items at a minimum?

A: Security Office Mission and Mandate Development, Security Office Governance, Security Policy, Development and Management, Security Training and Awareness Development, and Security Project Portfolio Development

Q: What is the purpose of incident response plans and procedures?

A: To provide a systematic approach as well as general guidelines for your staff on procedures to be followed whenever abnormal or unusual situations occur.

Q: What program provides the tools and measurements needed to protect against cardholder data compromise?

A: Visa USA CISP.

Q: What is the purpose of the IRT?

A: The IRT is created to execute the IRP.

Q: What is the purpose of testing the IRP regularly?

A: When an IRP is executed, there is little room for error. Testing makes it possible for methodologies to be developed that allow for timeliness and accuracy.

Q: What should you do if you determine your PCI data or a system has been compromised?

A: As a Visa member, you must seek the professional help of a QIRC to perform a forensic investigation.

Q: What is the benefit of using proper forensic techniques?

A: You will avoid costly discovery motion practices and allow you to gather and preserve the right data at the right time using early computer discovery planning tools. You will also avoid the traps of improperly mishandling, identifying, and preserving computer data.

Q: What does the CISP require you to do immediately after determining a security incident has occurred?

A: Immediately report security incidents and the suspected or confirmed loss or theft of any material or records that contain cardholder data.

Q: When should customers be notified of an incident?

A: Customer notice should be provided whenever it becomes aware of an incident of unauthorized access to customer information and, at the conclusion of a reasonable investigation, determines that misuse of the information has occurred or it is reasonably possible that misuse will occur.

Q: How should customers be notified of an incident?

A: A customer notice should be delivered in a manner designed to ensure that a customer can reasonably be expected to receive it.

Q: What is the penalty for failing to notify Visa USA Fraud Control immediately after an incident occurs?

A: $100,000 per incident if the member fails to immediately notify Visa USA Fraud Control of the suspected or confirmed loss or theft of any Visa transaction information,

Q: What is the penalty for being non-compliant with the PCI DSS at the time of an incident?

A: $500,000 per incident, if it is determined that the service provider is not compliant at the time of the incident.

Q: Why is BC/DR planning essential?

A: To provide the continuation of services to your customers in the event of unexpected occurrences that seriously disrupts the business process,

Q: Besides the recovery of technology and information, what other purpose does BC/DR planning provide?

A: BC/DR planning is also about maintaining, resuming, and recovering the business.

Chapter 12

Planning to Fail Your First Audit

Solutions in this Chapter:

- Remember, Auditors Are There to Help You
- Dealing With Auditor's Mistakes
- Planning for Remediation
- Planning for Retesting

- ☑ Summary
- ☑ Solutions Fast Track
- ☑ Frequently Asked Questions

Introduction

Whether it's your first on-site audit or your first external vulnerability scan, it's pretty easy to fail your first audit. And while this may not be the case for you, you should have a plan in place to deal with this if it happens. This may happen because you understood a requirement differently than what the auditor required, or it may be that you simply missed something. It's important to be prepared for this. As in all walks of life, whenever anything goes wrong we want to pass the buck. In this case, many times it's easy to pass the blame to the auditor. Having the right attitude came make all the difference. Generally, auditors are not going to be easy on you, because if they are too easy and don't correctly require companies to meet compliance, they can lose their auditing license.

Remember, Auditors Are There to Help You

When dealing with on-site auditors or approved scanning vendors, most people fit into one of three groups. Some people are intimated by auditors. They see them as someone with a lot of power, and they hope they will say and do the right things to get by. A second group seems to look at auditors as their enemy. They believe they must wrestle with the auditor and hopefully win in the end. The last set of people treat the auditor like a consultant they've brought in to help bring their company into compliance. They respect the auditor's opinions and keep the auditor in the loop as they work out solutions. This last group will get the most out of their auditor and will have the best overall experience and be able to bring their company into compliance with the least amount of hassle.

As hard as it might be to believe, auditors are there to help you. It's important to know how to work well with auditors so that your audit will go smoothly and efficiently, and ensure that you get your money's worth. A good auditor will go over your company's systems, practices, and policies with a fine-toothed comb, and tell you what you can do to improve your security. Hopefully, your primary goal in becoming PCI compliant is to have your company become more secure. When you realize that auditors provide you with a valuable service and that you're both on the same team working towards a common goal, you will have the right attitude. Remember that auditors have moral and professional obligations to follow the guidelines and procedures they've been given for the audit. It is not appropriate to ask them to compromise those obligations. Auditors are trained and likely have per-

formed many audits, and they can give you great advice on what you can do to bring yourself into compliance.

When you have the right attitude you will find ways to use your auditor to improve the security of your company. Seasoned auditors have a wealth of knowledge and can be a huge benefit to you to leverage it when bridging gaps in compliance. They have seen many technologies, policies, and practices others have put into place to mitigate risks, and should be able to give you choices to help you meet requirements that work best for your situation. For example, if cost is your main concern, an auditor may know of a low cost or open source tool that you can use to help you comply with certain requirements. On the other hand if time is more important, the auditor may know of a solution that is quick to set up that will bring you into compliance. As you work on your remediation, it's important to keep your auditor in the loop. This way he can give opinions on what you've chosen to do and can give further advice. It will also likely make your next audit much easier for both parties involved.

Tools & Traps…

Balancing Remediation Needs

It is important to do your homework when looking at ways to bridge compliance gaps. Depending on the problem you're trying to solve, there may be open source tools, managed solutions, off-the-shelf software, or hardware appliances that you may want to consider. When looking at products and services that can help bring you into compliance, there are usually four main factors that you should consider.

- **Effectiveness** Will the solution you're looking at really solve the problem and allow you to pass your next audit? If it won't, it should be ignored.
- **Cost** Normally cost is a factor in any decision made by a business. Sometimes decisions are based solely on initial cost, but costs of maintaining should also be considered. While one product is cheaper up front, it may end up costing your organization much more in the long run.

Continued

- **Time to Install** You likely want to be in compliance quickly. If you're not in compliance you will likely have gaps in your security that need to be filled to keep hackers out.
- **Time to Maintain** Many times, the time used to maintain a product will be the most expensive part of adding it to your organization. It may end up that a solution you choose will be more expensive in the long run, because it takes a lot of time to maintain.

Depending on your exact situation, some of these may be more important than others, but they should all be considered when choosing a solution.

In some cases, failing an audit ends up being a huge win for the security of the company. In many organizations, the IT staff would like to put certain needed security measures in place but upper management says no because of cost. Remember, upper management's job is to help the company make money, not spend money. Even after you have done a careful cost-benefit analysis and have determined that the benefits outweigh the costs, upper management may still say no. A failed audit may be the perfect time to finally get them to say yes. If the auditor is requiring that you add something to come into compliance, you can use it as leverage with upper management to get that put in place. Again, submit a cost-benefit analysis, adding the cost of noncompliance to the total cost. Let them know that the auditor says you will not be compliant without that measure.

Dealing With Auditor's Mistakes

Auditors are human and will sometimes make mistakes. This rarely happens, but if it does there is a right way to deal with it. The first thing to do is to talk to the auditor and have him explain how he came to his or her conclusion. Many times the customer misunderstood a requirement or believed a compensating control mitigated a problem, but the auditor doesn't agree. Having good open dialogue about what you believe is a mistake, will often solve the problem quickly.

Sometimes an auditor will report a false positive. This is when an audit shows you have a vulnerability such as a missing patch or vulnerable system that really is not there. This seems to happen more with remote scans, since they have less access to systems, but even then they are very rare. Any good auditor knows how to keep false positives to a minimum. When you do get a false positive, your auditor should be able to work it out with you. They may want to get more details from you so they

can verify that it is a false positive, and so they can fix the system so that they don't repeat them in the future.

Are You Owned?

Determining

Some approved scanning vendors basically run automated tools and do very little human checking. This generally works very well most of the time, but sometimes the scans can be very complicated, and because of some abnormality in your systems or something that happened during the test, a false positive occurs. Whenever you get a report that says you have a serious vulnerability, you should act as if it's true and see if there's something you can do to remediate the problem quickly. Depending on the situation, it may be a good idea to do some tests on your own. For example, the free tool Nessus has many of the same tests that an external scan will do. Depending on the type of vulnerability that was reported, you may be able also do some manual testing. For example if it's reported that a patch is missing, you may want to manually check on the system to verify if it is or is not. If after your testing you are unable to find the vulnerability, it may be time to challenge your scanning vendor's findings and report it as a false positive. They should do additional tests to determine why the false positive happened, and fix the problem for the future.

In some cases, you may need to push back. Pushing-back is when you challenge the auditor's results. This may happen because the auditor made a mistake, or because you don't feel like he adequately considered a mitigating control you had in place. When you push back you should be polite. Simply explain to the auditor your point of view and why you believe there was a mistake. If the auditor disagrees, ask him to explain his reasoning. If the auditor has explained why you didn't pass and you don't agree with his reasoning, you may need to talk to his manager about the situation. Normally, an auditor's manager will be a seasoned auditor who knows the process forward and backward. Explain your situation to the manager and why you think a mistake was made. Most of the time, the manager will talk to the auditor to get his side of the story before coming to any conclusions. If the auditor's manager agrees with the auditor, you will need to fix the problem to be compliant. Your only other option at this point is to find another auditor or scanning vendor. Usually the only

reason to do this is if you feel the auditor is blatantly wrong. However, an auditor from a different company will likely come to the same conclusions.

NOTE

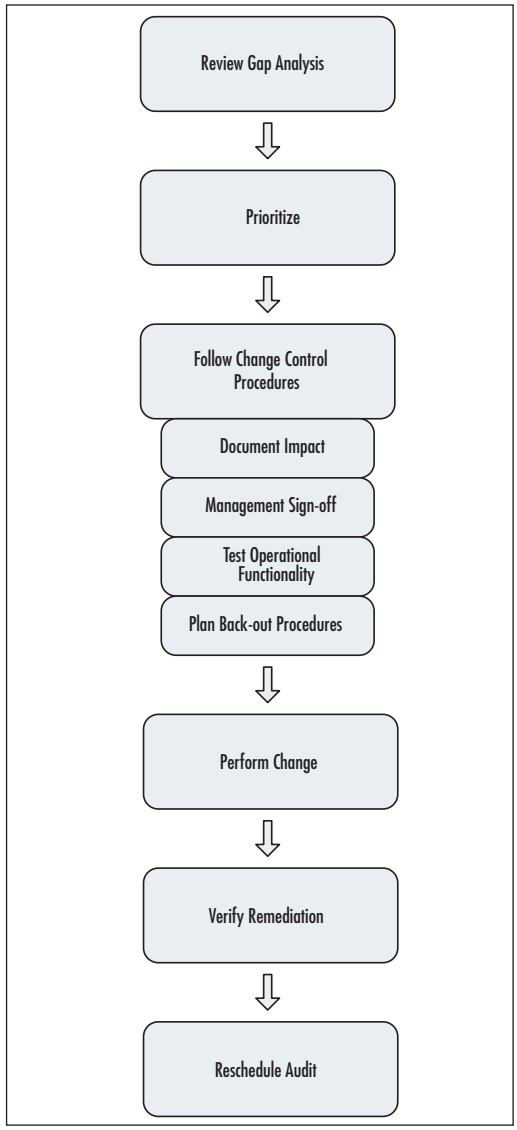
You may feel like you have mitigating controls in place to solve a problem but the auditor doesn't agree. In this case, it's the auditor who decides if a mitigating control mitigates the risk in question. The mitigating control should be at least as good, if not better, than what the requirement requires. Most of the time it's easier to follow the requirement exactly than to try to get a mitigating control to fix the problem.

Planning for Remediation

A good rule of thumb when doing remediation is that it should be as transparent as possible, so that it has a minimal impact on users. There may be times that remediation may have some impact on users. For example, implementing a much stricter password policy or disabling group accounts may have an effect on how users do their jobs. For the most part, patches and system updates should be transparent to users. The more transparent your remediation, the less problems you're likely to have implementing it. As you plan your remediation process, always keep transparency in mind.

The first thing you should do in planning for remediation is review your compliance gap with your auditor. Your compliance gap describes the difference from where you are now and where you should be to be compliant. You should get a report and be briefed on the details of the problems. It is important to ask your auditor which risks he considers high priority. For example, if the auditor feels that you have urgent risks that could easily be exploited at any time, you would want to work on mitigating these first. In a few cases, an auditor will find a risk that is being actively exploited. In this case, the auditor should let you know as soon as he finds the problem and not wait until the rest of his assessment is done. This would then become your top priority, and you should follow your company's procedure for dealing with attacks and call in your incident response team.

Figure 12.1 Remediation Process



Now that you have your results and understand what needs to be done to come into compliance, it's time to prioritize our risks. With the help of your auditor and by doing your own research, you should work to determine which problem can be exploited easiest and can cause the most damage. These are the ones that should be fixed first. There are many tools that can be used to help you classify risks, including the many vulnerability Web sites. Here are some that you might find useful

- **Common Vulnerability and Exposures (CVE)** This is a well-respected and much referred to listing of vulnerabilities in products. Many products use CVE number to reference vulnerabilities (http://cve.mitre.org/).
- **National Vulnerability Database** Supported by the Department of Homeland Security and has a great database of many types of vulnerabilities (http://nvd.nist.gov/).
- **Open Source Vulnerability Database (OSVDB)** A community run database of vulnerabilities. It will give you a lot of great information on a vulnerability, including references, ways to test your system, and how to mitigate the problem (www.osvdb.org).
- **Security Focus Bugtraq** A well-organized site that will give you a lot of information including what versions are effected, an overview of the problem, and examples of exploits. It uses Bugtraq IDs (bids) which are supported in many products (www.securityfocus.com/bid/
- IBM Internet Security Systems (ISS-XForce) A site backed by IBM that gives great overviews of many vulnerabilities (http://www.iss.net/).
- **Secunia** A Danish computer security company that lists and prioritizes vulnerabilities (http://secunia.com/).

Tools & Traps…

Common Vulnerability Scoring System (CVSS)

CVSS is a standard for scoring vulnerabilities that is become more widely used. Approved scanning vendors should start using CVSS scores rather than the PCI scores starting June 30, 2007, for any vulnerabilities that have a CVSS score. Most of the vulnerability databases will list CVSS scores, which are great in helping you determine the impact of a vulnerability. There are some vulnerabilities that may not have a CVSS score, but NIST provides a great tool to help you calculate them, which can be found at http://nvd.nist.gov/cvss.cfm?calculator.

For example, let's say that your report shows that you don't have your credit card area physically secured. Since this is not a specific vulnerability with a specific system, there won't be a CVSS score for it, but you can use CVSS to help you determine the priority.

Continued

In this example, we'll use a physical security issue to show you how this works. While this system is mainly for computer security issues, it works pretty well for physical vulnerabilities as well. Say your organization has a fax machine in a public area (such as a store lobby) where faxes containing orders that include cardholder data are received. Let's say that the location is not always closely monitored. For example, there may be times when the employees in the lobby are busy with customers and aren't watching the fax machine and therefore anybody could grab a fax.

On the calculator page, you would start with the Base Scoring Metrics. This gives CVSS a base score to work of off for the vulnerability.

Related exploit range is where an attacker would have to be to be able to exploit this vulnerability. If an attacker can compromise the system over the Internet or some other remote means, then it would be remote. In our case, with the credit card area not being physically secured properly, it would be **Local**.

Attack complexity is how hard it is to pull off the attack once an attacker has found the vulnerable target. If the attack requires other factors to be in place for it to work, it may make it complex. In our case, we'll say that this is **Low** complexity. Once an attacker knows where the credit card data is, it's easy for them to get to it, because our physical security is so bad.

The level of authentication needed is if an attacker must be authenticated to pull off an attack. This means that there is a test to verify who the user is that they have to bypass to attack the system. An example would be if to pull off our attack against the area with credit card data, we needed a fake badge. We're going to say that we don't (we can just walk in nobody will stop us) so the level will be **Not Required**.

Confidentiality impact is how the exploit will affect confidentiality of data that should be protected. In our case, if they can access cardholder data by simply walking into a protected area and walking off with a file cabinet with all cardholder data in it, it would be complete. We'll say that the filing cabinet is pretty safe, but we have faxes that come in with cardholder data on it and we don't protect it. In this case the confidentiality impact would be **Partial**.

Integrity impact is how the attack will impact the integrity of data. In our case, it's not likely that integrity will be compromised, so we'll use **None**.

Availability impact is the measure of how it will affect the availability of systems and data. Since the attacker can walk off with a fax, the data is no longer available, so we'll mark that as **Partial**.

Impact value weighting allows you to give more weight to confidentiality, integrity, or availability. In our case, the biggest problem will be confidentiality, because the attacker just walked off with cardholder data, so we will chose **Weight confidentiality**.

Continued

At this point if we click **Update Scores**, we will get a base score of 3.7.

Now we will do the temporal score metrics.

Availability of an exploit lets you determine if an exploit is actually available or not. In our case, we'll say that a **Functional exploit exists** since the attack would work much of the time, but there may be times when an employee would catch somebody.

The type of fix available allows us to specify if there is currently any way to remediate the problem. We'll say that we've asked employees to keep an eye on the fax machine, which is a **Temporary fix** until we find a better place to move the fax machine to.

Level of verification that the vulnerability exists allows us to specify how sure we are the vulnerability is actually there. In our case, we know that the vulnerability exists so we'll choose **Confirmed**.

Now on to the environmental score metrics section. Here we will look at what kind of damage will happen.

Organization-specific potential for loss allows you to specify the physical impact the attack could have on your systems. In our case, one credit card number stolen on a fax likely won't bankrupt the company, so we'll say it has **Low (light loss)**

The percentage of vulnerable systems allows us to choose how many of our systems are vulnerable to this attack. In our case, this is our only fax machine so we'll say all of them and chose **High (76 to 100 percent)**.

Now that we're done, we click the **Update Scores** button and get an overall score of 3.9.

There are many ways to prioritize risks, depending on how many and what types they are. You may want to use a simple or complex system for this. You should not spend a huge amount of time and effort prioritizing risks, since in the end they all need to be fixed. But it's good to have a general idea. We will discuss a quick way here and in the side bar titled CVSS, and we will discuss a slightly more complex way. We will score all vulnerabilities on a scale of 1 through 5 (5 being the worst) for risk level and probability of attack. We will then use these numbers to prioritize which ones to fix first.

NOTE

If you have a few gaps that will be remedied quickly, this quick classification system works best. If you have several vulnerabilities, some of which will take a long time to work out, then it's probably best to use the CVSS.

First we will classify vulnerabilities on a scale of 1 through 5 based on how bad these vulnerabilities are.

- **5** Urgent vulnerabilities that should be fixed as soon as possible. Basically this is when your system has been compromised and you should work to quickly get this fixed.
- **4** Critical vulnerabilities that have not been used to exploit your system yet, but may be in the near future. An example of this could include a patch to your systems are missing and there is a known worm crawling the Internet exploiting this problem. While this is not as bad as a system that is currently compromised, it's a close second and should be fixed soon.
- **3** High risk vulnerabilities that could be serious if exploited, but there is no worm or prolific exploit. An example of this might be a vulnerability that could be exploited by a script kiddie level malicious user.
- **2** Medium level vulnerabilities are ones that would require a very sophisticated attacker to pull it off, but it's still possible. This could include a situation where a vulnerability is partially mitigated or there is a temporary fix in place.
- **1** Low severity vulnerabilities, which include information disclosure or other type of vulnerability that doesn't pose much of a risk by itself, but if used with other information, may be exploited.

Next, we will give vulnerabilities a score of 1 through 5 based on the loss your organization will suffer if the vulnerability is exploited. When using this system, you should consider all forms of financial losses including loss of customers, cost to fix the problem after it happens, and so forth.

- **5** The business will go bankrupt and no longer exists. You will not be able to survive a compromise of this kind.
- **4** This likely won't shut the company down, but will have significant impact on the company financially.
- **3** Your company will suffer a medium amount of loss. This will still be bad for the company, but they should be able to weather it without much problem.
- **2** Your company will suffer a small but noticeable loss financially.

- **1** The financial loss if this were exploited, would not really be noticed.

Now that we have classified all of our vulnerabilities based on the two systems, all you need to do is add up the two numbers for each vulnerability and you have its priority. Let's do an example to show you how this is done. Let's say that we have a vulnerable Web server. There is no worm that is actively crawling the Internet exploiting this problem, but there is exploit code available that is easy to use. In this case, we would give the vulnerability a severity risk of 3. Looking at the possible loss, we decide that it could be a pretty big deal. If an attacker was able to compromise our Web servers they could steal all incoming credit card information and could possibly use the Web server to get to other computers in the DMZ. There is also a possibility that an attacker can perform a pretty significant Denial of Service (DoS) attack against the Web servers. This would cost a decent amount of money, but wouldn't put us out of business. It's also important to consider penalties that could be levied because of PCI non-compliance. All of this considered, we decide to give the vulnerability a loss rating of 4. Now we simply add 3 and 4 and this vulnerability's priority is 7. The highest possible vulnerability is 10 (even though this would mean that a vulnerability is being actively exploited that will almost certainly result in your company going bankrupt).

TIP

After you've followed some system for prioritizing vulnerabilities for awhile, your instinct will tell you to fix one or more out of order. It's usually not a bad idea to follow your instinct.

Now that you have prioritized vulnerabilities, you should start fixing them from highest to lowest. You should have a change management policy in place and use that policy when you are implementing the changes. To be compliant with PCI, your policy should include several parts. For example, before you implement any change, you should document the impact the change will have on all users and customers. This should include any behaviors that users will have to change, or anything that will work differently after the change is made. It is important that you always remember to have management sign off before you make any of the required changes, to bring yourself into compliance. You should also always remember to test your change in a test environment before putting it into production. This is impor-

tant to verify that it doesn't introduce other problems that must be resolved before you put it into production. You must also always have a back-out procedure in place just in case the change causes problems. After you have everything in place, make the update and then make sure you update any applicable documentation.

Before your retest, it's a good idea to test your changes as best you can to verify that they are working as planned. For changes to systems, there are many tools that can help you do this. Nessus is a really good free vulnerability scanner that you can use to test for missed patches and other misconfigurations on many different systems. You may want to look at the Self Audit section in Chapter 13 for more suggestions on testing yourself.

WARNING

Before running any type of scan on your network, you should always get management's approval.

Planning For Your Retest

As you are working through mitigating your risks and bridging the gaps to compliance, you should include the auditor as you go along. Not only can he give advice on how to mitigate some risks and bring yourself into compliance, he or she will also likely be able to help you set realistic dates to work towards. As you run into road blocks, he or she can help you readjust these dates and give you further advice.

After this is done and everything is in place, you should have your retest planned to happen soon. Having worked with your auditor during the remediation process, your retest should be quick and painless and then you will have that coveted paper that shows that you're compliant.

Summary

Don't feel bad if you fail your first test. Instead, use it to your advantage to increase your company's security posture. It's important to work with auditors instead of against them. Remember you and your auditor are on the same team and aren't working against each other. By doing what you can to follow your auditor's recommendations, your audit should be less painful and work much more quickly. You should involve our auditor as you work to bridge the gap in your compliance. The more you involve the auditor, the easier your retest will be.

Solutions Fast Track

Remember Auditors Are There To Help You

- ☑ Have the right attitude when dealing with auditors.
- ☑ Remember your auditor has experience and knowledge that can help you.
- ☑ Get advice from your auditor on how to bring yourself into compliance.

Dealing With Auditor's Mistakes

- ☑ Mistakes should be rare.
- ☑ If you believe there is a false positive, you should talk it over with your auditor and possibly do tests on your own.
- ☑ You may need to push back and possibly get the auditor's manager involved if you believe the auditor is not being realistic in the audit.

Planning For Remediation

- ☑ Review your compliance gaps with your auditor.
- ☑ Prioritize your risks so you can fix the most pressing first.
- ☑ Follow your remediation process when implementing changes to bring yourself into compliance.
- ☑ Test yourself to verify.

Planning For Your Retest

- ☑ Include your auditor in all parts of the remediation process.
- ☑ Work to get retested in a timely manner.

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to **www.syngress.com/solutions** and click on the **"Ask the Author"** form.

Q: Do I really need to prioritize risks since I need to fix them all to become compliant. Can't I just fix them in a random order?

A: While you do need to fix them all, it's a good idea to fix them according to priority, especially if there are some that are high risk. Remember, you're working to protect your company and customers against cardholder data being stolen. When you're fixing problems, you should fix the ones that can cause the biggest problems and that are the easiest to exploit first, giving the protection you need sooner.

Q: Under what circumstances should I find another auditor?

A: It is very rare that you should change auditors. If you are thinking about changing auditors because yours doesn't accept your compensating control (which is sketchy at best), don't do it. If one auditor doesn't accept it it's likely another one won't either. The best thing to do is to take the audit seriously and work to make your systems more secure. Normally, the only reason to find a different auditor is if you simply cannot work with the one that you have.

Q: I don't want to fail again. What's the best way to ensure I pass my retest?

A: Working closely with your auditor and involving them in the remediation process will likely be the single most important thing you can do to ensure you pass your retest. As you work through risks and remediation on each of them, talk to your auditor about their opinions.

Chapter 13

You're Compliant, Now What

Solutions in this chapter:

- **Security is a PROCESS, Not an Event**
- **Plan for Periodic Review and Training, Don't Stop Now!**
- **PCI Self Audit**

- ☑ **Summary**
- ☑ **Solutions Fast Track**
- ☑ **Frequently Asked Questions**

Introduction

Congratulations, you passed! Depending on where you were when you started, you may have worked long and hard to get here. So now you can kick back, relax, and wait until your next annual audit, right? It would be great if it were that easy, but unfortunately it's not. Security (and Payment Card Industry [PCI] compliance in particular) requires constant maintenance. In this chapter we will discuss how you can best spend your time now to ensure compliance in the future. First, we will discuss why you should think about security as a process instead of an event. We will then make suggestions on periodic review and training that should be happening in your organization. Last, we will outline some suggestions on performing a self-audit on your own network.

Security is a PROCESS, Not an Event

Security is not something that can be achieved, and then forgotten about. Contrary to some security vendor's claims and some management hopes, you cannot install some magical device on your network that will make you eternally secure. Security is a process of constantly assessing your risks then working to mitigate them to a reasonable level. These risks are ever-changing, so processes and technology to stop them should be ever-changing as well.

One thing to keep in mind is that you were never 100 percent secure to begin with. Even if you've done everything you can find to secure your systems, an attacker can still find ways in. In fact, it's actually very difficult to prove that you are secure and it's relatively easy to prove that you are insecure. To prove that you are secure you must prove that every possible risk (remember, these are constantly changing) is protected against. To prove insecurity you only have to find one attack vector that isn't fully mitigated against. This could be an attack vector that you have never thought of. It could be one that only one attacker in the whole world knows about, and if that attacker decides to target your company, then despite all you have done he could successfully attack your network. Also, the more complex a system is the harder it is to secure. It is very difficult to have a system that's completely secure that actually does something useful, like serve a Web page or allow a user to send an e-mail. In general, today's systems are very complex, and therefore hard to secure.

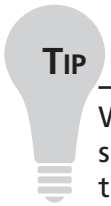
Second, risks, technologies, and your organization are changing constantly. New attacks are invented constantly. New technologies and software are implemented in your network on a regular basis. New people come to your company and current

employees likely forget things from time to time. To remedy this new security, measures need to be invented and people need to be trained regularly.

Third, it's impossible to be PCI compliant without approaching security as a process. All of the requirements require some sort of maintenance. Logs need to be reviewed, systems and policies need to be updated, and security assessments need to be run. These are all part of the security process that keeps your company as safe as possible from attacks.

Plan for Periodic Review and Training, Don't Stop Now!

It's important to plan now for future review and training. Working with technology in an organization can get very hectic, and if you put off planning then you are far less likely to do it. It's important to review your security polices and practices often to verify they're actually being implemented. Many times great policies are in place but never enforced and so they are never actually followed. It's also important to train your employees often to ensure that they understand and are reminded of your security policies. Periodic training also emphasizes the importance of security polices to employees so they're more likely to follow them.



TIP

We recommend training session that are brief and often. For example, a short 15-minute reminder session several times a year will likely be better than an hour-long review session once a year.

Here are some ideas of things you may want to review with employees at your organization:

- **Passwords** What makes a good password? Remind them never to share their password with anyone for any reason. Warn them of common mistakes such as writing passwords on a post-it note and sticking it on the computer monitor.
- **Social Engineering** Don't let people fool you. Make policies for visitors clear to ensure that a malicious visitor won't leave with information they shouldn't have. Also, you could review polices for verifying an employees

identity when they make requests (such as password resets) over the phone or in some other non-face-to-face situation.

- **Physical Access** Verify that everyone knows what a visitors badge looks like and knows what the company policies are with regards to where visitors are allowed to go and where they are not allowed to go.
- **Correctly Storing and Destroying Sensitive Material** Help employees keep up-to-date with company polices that require that sensitive data be destroyed. For example, it's important that employees are trained on destroying paper and electronic media that contains confidential data when it's not longer needed.

Your Information Technology (IT) staff also needs to be regularly trained on security. For example:

- **Secure Coding Practices** Software engineers don't necessarily need to be security experts, however, it's important that they understand secure coding practices. For example, anyone working on a Web application should be aware of cross-site scripting (XSS) and Structured Query Language (SQL) injection bugs. Programmers should also be aware of unsafe functions that may be available in their language, and their safer alternative functions.
- **Systems administrators** should be kept up-to-date with secure practices that are related to the systems they administer. They should know how to securely install and configure these systems.
- **Security professionals** at your company must be trained regularly. Depending on the size of your company, this may be a few or several employees. These are the people are responsible for securing your systems day in and day out. They must receive periodic training to help them be aware of new technologies and new attacks.

You should also regularly review the PCI requirements. You should choose a review schedule that doesn't take so much time that you will never actually get to it, but that allows you to review often enough that you will have PCI requirements fresh in your mind. We recommend that you set aside a certain day a month for your review. A good rule of thumb is to review all PCI requirements quarterly. Currently, this would mean four requirements a month, which should be easily manageable. Reviewing on this schedule should also keep you in great shape for your quarterly

scan and annual audit. This will also keep you up-to-date with any changes in the PCI requirements.

PCI Self-Audit

In this section we'll go over each PCI requirement and give some ideas on how you can audit each requirement to verify that you are currently in compliance. Often times when a company first becomes PCI compliant you have to make many changes to their current security policy. Because of this, it's very important to audit any new policy changes you've made to verify that they are working at your organization. This way you can find weak points in your policy or employee education that need to be addressed.

The PCI Security Council provides some great documents to help you with your self assessment. For example, the Self-assessment Questionnaire can help you determine your company's current compliance level. You should periodically review these documents, and look for ways to improve your company's security posture.

There are also many freely available and commercial security tools that can be used to test your company's level of compliance. For example, Nessus is a fantastic vulnerability assessment tool that is free and works on both Windows and Linux. There are also many great free port scanning tools such as SuperScan or Nmap. Many of these tools are available on a live Linux CD called Backtrack (www.remote-exploit.org/backtrack.html) that contains many tools to help assess network security. Several mini-tutorials are contained throughout the chapter on how to use some of the most important tools from this CD to help test your PCI compliance.

WARNING

You should always have permission from management before you run any type of scans on your systems. Unexpected things can happen when running these scans. For example, sometimes scans will cause printers to spew pages until they run out of paper. Worse, sometimes these scans can take down networks or critical systems. You may want to find a time when traffic is low to run these scans (e.g., late at night). This way any outage should cause minimal damage.

In the following section each requirement is broken up into two parts. Under the "Policy Checks" heading we discuss policies that should be reviewed to verify that

they are up-to-date. In the "Hands-on Assessments" sections we give some ideas on testing these policies to ensure that they have been properly implemented.

Requirement 1

Requirement 1 is about firewall and router configuration policies.

1.1 Policy Checks

Obtain a copy of the firewall and router configuration standards and verify it is up-to-date with your current configuration and that the following items are included:

- A policy for making changes to firewall configurations. This should include a testing procedure and a requirement that management signs off on any changes.
- An up-to-date network diagram of connections to all systems that deal with cardholder data. This should show a firewall at any Internet connection and between the demilitarized zone (DMZ) and internal network.
- A requirement that a firewall be placed at each connection to the Internet and between the DMZ and internal network.
- A description of groups, roles, and responsibilities for logical management of network components.
- Justification and documentation for any protocols being used besides Hypertext Markup Language (HTTP), Secure Sockets Layer (SSL), Secure Shell (SSH), and Virtual Private Network (VPN).
- Justification and documentation for using any risky protocols such as File Transfer Protocol (FTP).
- A procedure for a quarterly review of firewall and router rule sets.

1.1 Hands-on Assessments

Interview firewall and router administrators and verify that the change policy was followed in the most recent changes to the firewall configuration. Verify that management is signing off on changes to the firewall by obtaining and reviewing the signed forms. A great tool to help you audit your firewall compliance and check your network diagram is a port scanner such as Nmap or SuperScan. For example, you can run a port scanner on your network and compare the list of hosts returned by the

port scanner to your network diagram. While running a port scan on a network may not find all the hosts, it will at least find all the hosts with open ports. In section 1.2 we'll outline some methods for testing the firewalls between the Internet and your networks and between the DMZ and your internal network.

Tools & Traps…

Using Nmap

Fyodor's Nmap (http://insecure.org/nmap/ is a great vulnerability scanner with many options. We won't be able to cover Nmap in depth here, but we'll cover enough so you can do a basic scan on your systems.

Nmap can be installed on Windows or Linux. A great way to get up and running with Nmap is to use the Backtrack live Linux CD. After running *startx* the tool is found by clicking on **Backtrack | Scanners | Nmap**.

To syntax for Nmap is:

nmap [scan type] [options] {targets}

So to perform a simple *syn* reset scan against 10.0.0.1-10.0.0.5:

nmap –sS 10.0.0.1-5

To perform an syn ack scan against the same hosts:

nmap –sA 10.0.0.1-5

A very useful option is disabling pings, which would otherwise make Nmap skip hosts that don't respond to ICMP pings. You do this with the *P0* option. For example:

nmap –sS –P0 10.0.0.1-5

1.2 Policy Checks

Verify that policies are up-to-date that require firewalls between the Internet and DMZ and the DMZ and the internal network.

1.2 Hands-on Assessments

Run a port scanner against routers and firewalls that segregate the Internet from your networks and the DMZ from the internal network, to verify that these routers and firewalls are properly restricting traffic. For example, if you use a port scanning tool from the Internet against your network, it should only return ports appropriate to do business on your systems. If you find protocols other than HTTP, SSL, SSH, or VPN

being used, then they must be justified and documented in your firewall policy. If there is no business reason for these protocols, they should be disabled and a review should happen to determine how and why there were enabled. You should also inspect the configuration on firewalls on a regular basis to ensure they are properly configured as prescribed in your firewall policy.

1.3 Policy Checks

Verify that you have an up-to-date policy that requires the following configuration settings on firewall and routers between publicly accessible servers and systems (a wireless network is considered a publicly accessible network) and systems storing cardholder data.

- Traffic from the Internet is only allowed through the firewall between the Internet and the DMZ if the destination IP addresses is within the DMZ.
- Internal IP addresses in the DMZ must be filtered by firewalls so they are not allowed to flow from the DMZ to the Internet.
- Stateful packet filtering (also called dynamic packet filtering) must be enabled on all firewalls.
- Databases storing credit card data must be on the internal network and not in the DMZ.
- Only traffic that is required to conduct business should be allowed in and out of your network. Your firewall should restrict all other traffic.
- Router and firewall configuration files must also be synchronized and up-to-date. Verify that running configurations and start-up configurations are the same for all routers and firewalls. This means that when you reboot your routers and firewalls, they will be using the same configurations they were before the reset.
- By default all traffic in and out of your network should be explicitly denied, and then only protocols required to do business should be allowed.
- A firewall must exist between any wireless networks and internal networks that store cardholder data. Check your network diagram discussed in Requirement 1.1 to verify that this firewall is on your diagram.
- Any company-owned mobile computer or employee-owned computer must have a personal firewall installed on it, which must be configured to comply

with your company firewall standards. It must also be configured in such a way that the employee cannot alter the configuration.

1.3 Hands-on Assessments

Examine your firewalls and routers between the Internet and the DMZ to verify that they only allow traffic through, and that their destination Internet Protocol (IP) is an IP in the DMZ. Examine these configurations to ensure internal DMZ addresses are filtered from passing back out to the Internet. You can test to see if stateful packet filtering is working by using Nmap on all Transmission Control Protocol (TCP) ports with syn reset or syn act options set. If you receive a response, then stateful packet filtering is not properly enabled. You should also examine the configuration of your database server to verify that a firewall exists between it and the DMZ.

You can run a port scan to verify that only protocols required for business are allowed through the firewall. Take a sample of the firewall and router configurations to verify that they are up-to-date and that the running configurations match the boot-up configurations. Verify that firewalls rules start with an explicit deny all, and then only protocols needed for business are enabled. Examine wireless connections in your network to verify that a firewall is installed between the wireless network and any network where wireless data is stored. Take a sample of mobile and employee-owned systems to verify that a software firewall is installed and enabled, and that the settings cannot be altered by the employee.

1.4 Policy Check

Your firewall policy should mandate that not direct access is made between the external network and internal computers that store credit card data. Also, it should mandate that outbound traffic from payment card applications be restricted to only go to IP addresses in the DMZ.

1.4 Hands-on Assessment

Check firewall policies to verify that no direct (non-firewalled) access to systems within the internal network is allowed. Examine firewall and router configurations to verify that traffic from the internal network is only allowed to access IP addresses within the DMZ.

1.5 Policy Check

Your policy must require that your firewall use IP masquerading to block RFC 1918 address space from traveling from internal networks to the Internet.

1.5 Hands-on Assessment

Review firewall configurations to verify that network address translation (NAT) or other technology is used, which restricts broadcasting RFC 1918 IP addresses from the internal network to the Internet.

Requirement 2

Requirement 2 verifies that you are not putting systems live with default security settings.

2.1 Policy Checks

Verify that your policy requires that system defaults must be changed before you install a system on the network. This includes settings such as passwords, Simple Network Management Protocol (SNMP) community strings, removal of unnecessary accounts, and so forth. Your policy must also require that vendor defaults for wireless devices are changed before they are placed on the network.

2.1 Hands-on Assessment

Nessus includes several plugins that will try to use default accounts to log into systems. Alternatively, you may want to either attempt to log in manually using default passwords, or use a tool such as THC-Hydra to do this for you. For wireless networks there are several tools such as Netstumbler and Kismet that will find some default configurations. For example, you can use these tools to find access points that are not using encryption or that are broadcasting default Service Set Identifier's (SSIDs). It's also important to check the configuration on these devices to verify that they are correct. For example, you could take a sample of wireless access points and verify that they are using non-default Wireless Encryption Protocol (WEP) keys (if WEP is enabled). You should also verify that SSID broadcasting is off and they are not using the default SSID. The SNMP community strings on wireless access points must also be changed from the default. If possible, Wi-Fi Protected Access 2 (WPA2) or Wi-Fi Protected Access (WPA) should be enabled on all access points (whenever possible

WPA2 should be used). Verify that if there are other security-related default settings on the wireless access point, that they are changed from the defaults.

Tools & Traps...

Using Kismet

Kismet (www.kismetwireless.net) is a wireless network analyzer that runs on Linux. It is included on the Backtrack CD. To start Kismet click on **Backtrack | Wireless Tools | Analyzer | Kismet**. If your card is compatible and everything worked right you should see Kismet's window pop up. It will automatically start to find any wireless networks in the area. You can then walk around your organization and it will log all wireless networks it finds.

2.2 Policy Checks

Your configuration standards for systems in your network must be up-to-date with the following:

- Current industry-accepted hardening standards for your systems from industry-respected organizations including SANS, NIST, and CIS.
- Require that only one primary function is implemented per server (e.g., you cannot be running a primary Web and primary database server on the same machine).
- Require that all insecure services or protocols, or those services or protocols not required for that system to perform its functions, should be disabled.
- Require that system security parameters are configured to lock down the system as much as possible.
- Require that all unnecessary functionality is removed from systems, such as scripts, drivers, Web servers, and so forth.

2.2 Hands-on Assessments

You should take a sample of systems in your organization and verify they are compliant with your policy. For example, you should take a sample of critical servers or

wireless access points and verify that only one primary function is implemented per server. You should take a sample of system components, critical servers, and wireless access points and inspection-enabled services, daemons, and protocols. You should verify that only necessary services and protocols are enabled. You should also interview and work to educate system administrators on things they can do to lock down systems. For example, verify that security parameter settings are set correctly for each system. Also verify that all unnecessary components such as driver scripts and so forth are removed. There are many network assessment tools that will help you do this, including Nessus. Microsoft Baseline Security Analyzer can also be very helpful in assessing basic lockdown settings on Windows machines.

2.3 Policy Checks

Verify that your policy requires all non-console initiative access be encrypted. For example, your policy should require that SSH, VPN, SSL, or similar technology is used instead of unencrypted HTTP, Telnet, or other unencrypted protocol.

2.3 Hands-on Assessments

Take a sample of systems on your network and have the system administrator's log into various accounts remotely while you observe them. Verify that they are using SSH or other encrypted protocol to manage these systems remotely. Also examine system configurations to verify that Telnet and other insecure administrative services are disabled on systems on your network.

2.4 Policy Checks

If you are a shared hosting provider, your policy must require that each entity's hosted environment and data are protected. You should also have a policy in place that outlines how to perform a timely forensics investigation if a system is compromised.

2.4 Hands-on Assessments

This requirement only applies to hosting providers. If you are a hosting provider, then you should examine the configuration of your systems to verify that a user only has access to their own cardholder data environment. For example, no entity should be using a shared Web server user ID. Also, each user's Common Gateway Interface (CGI) scripts must be created and run as a unique user. Verify that no application process is run using a privileged user account such as Administrator. Verify that each

entity only has permissions to read, write, and execute their own files and directories and required system files. Sometimes users need read permission to certain system binaries, if required, but they should never have write permission. Inspect the configuration to verify that reading log entries is restricted to the entity that owns them. Inspect the systems to verify that restrictions are in place to prevent a single user from monopolizing the systems, such as using up all the disk space, memory, bandwidth or central processing unit (CPU). Verify that logs are being kept of all actions taking place on the system.

Requirement 3

Requirement 3 is used to ensure that cardholder data is protected when it is stored on you systems.

3.1 Policy Checks

Verify that your policies and procedures are up-to-date with the following items:

- Specify how long credit card data needs to be kept and specify the legal, regulatory, and/or business reasons for the specified length. The length specified should be the minimum amount of time needed to meet legal, regulatory, and/or business reasons.
- Coverage of all cardholder data storage should be included. For example, secure data storage on mainframes, database servers, transfer servers, and so forth should be included in the policies and procedures.
- A description of an automatic process in place removal of the data was no longer needed.

3.1 Hands-on Assessments

Take a sample of systems that store cardholder data including mainframes, database servers, transfer servers, and so forth. Verify that data is being stored for exactly as long as your policy directs. Also verify that your automatic process for removal of cardholder data is working correctly by sampling systems and verifying that data is removed.

3.2 Policy Checks

Verify that your policy includes the following in relation to sensitive authorization cardholder data:

- If the sensitive authorization data is received then deleted, it must be deleted in a secure way that renders it unrecoverable.
- The full contents of the magnetic strips must never be stored.
- The 3- or 4-digit card validation code (sometimes called the CVV2, CVC2, CID, or CAV2) must not be stored after the card is authorized.
- The personal identification number (PIN) or encrypted PIN block must not be stored after the card is authorized.

3.2 Hands-on Assessments

Either manually or using log parsing tools, you should look through transaction logs, history files, trace files, debugging logs, as well as incoming transaction data, several database schemas, and the database content to verify that sensitive authorization data is not being stored after authorization of the card is complete. Sensitive authorization data includes the full contents of the magnetic strip, the 3- or 4-digit card validation code, and the PIN.

Tools & Traps…

SQL Server Stored Procedure for Finding Plain Text Credit Card Numbers

The following is a stored procedure to help you locate any credit card numbers stored in plain text in your SQL Server database. Similar things can be done in MySQL and Oracle. This stored procedure will find VISA, MasterCard, American Express, Discover, and Diners card numbers. Note: this will likely find several false positives; it will be up to you to determine if what is returned is a plain text credit card number of a false positive.

```
SET ANSI_NULLS ON
GO
```

Continued

```
SET QUOTED_IDENTIFIER ON
GO
CREATE PROCEDURE [findCCNums]
AS
BEGIN
    CREATE TABLE #CCRes (ColName nvarchar(370), ColValue nvarchar(3630))

    SET NOCOUNT ON

    DECLARE @TableName nvarchar(256), @ColName nvarchar(128), @VISANoExtras
nvarchar (256), @MCNoExtras nvarchar (256), @DISCNoExtras nvarchar (256),
@AMEXNoExtras nvarchar (256), @DINNERSNoExtras nvarchar (256), @VISAdashes
nvarchar (256), @MCdashes nvarchar (256), @DISCdashes nvarchar (256),
@AMEXdashes nvarchar (256), @DINNERSdashes nvarchar (256), @VISAspaces
nvarchar (256), @MCspaces nvarchar (256), @DISCspaces nvarchar (256),
@AMEXspaces nvarchar (256), @DINNERSspaces nvarchar (256)
    SET @VISANoExtras =
'4[0123456789][0123456789][0123456789][0123456789][0123456789][0123456789][0
123456789][0123456789][0123456789][0123456789][0123456789][0123456789][01234
56789][0123456789][0123456789]'
    SET @MCNoExtras =
'5[12345][0123456789][0123456789][0123456789][0123456789][0123456789][012345
6789][0123456789][0123456789][0123456789][0123456789][0123456789][0123456789
][0123456789][0123456789]'
    SET @DISCNoExtras =
'6011[0123456789][0123456789][0123456789][0123456789][0123456789][0123456789
][0123456789][0123456789][0123456789][0123456789][0123456789][0123456789]'
    SET @AMEXNoExtras =
'3[47][0123456789][0123456789][0123456789][0123456789][0123456789][012345678
9][0123456789][0123456789][0123456789][0123456789][0123456789][0123456789][0
123456789]'
    SET @DINNERSNoExtras =
'3[068][0123456789][0123456789][0123456789][0123456789][0123456789][01234567
89][0123456789][0123456789][0123456789][0123456789]'

    SET @VISAdashes = '4[0123456789][0123456789][0123456789]-
[0123456789][0123456789][0123456789][0123456789]-
[0123456789][0123456789][0123456789][0123456789]-
[0123456789][0123456789][0123456789][0123456789]'
    SET @MCdashes = '5[12345][0123456789][0123456789]-
[0123456789][0123456789][0123456789][0123456789]-
[0123456789][0123456789][0123456789][0123456789]-
[0123456789][0123456789][0123456789][0123456789]'
    SET @DISCdashes = '6011-
```

Continued

```
[0123456789][0123456789][0123456789][0123456789]-
[0123456789][0123456789][0123456789][0123456789]-
[0123456789][0123456789][0123456789][0123456789]'

   SET @AMEXdashes = '3[47][0123456789][0123456789]-
[0123456789][0123456789][0123456789][0123456789][0123456789][0123456789]-
[0123456789][0123456789][0123456789][0123456789][0123456789]'

   SET @DINNERSdashes = '3[068][0123456789][0123456789]-
[0123456789][0123456789][0123456789][0123456789][0123456789][0123456789]-
[0123456789][0123456789][0123456789][0123456789]'


   SET @VISAspaces = '4[0123456789][0123456789][0123456789]
[0123456789][0123456789][0123456789][0123456789]
[0123456789][0123456789][0123456789][0123456789]
[0123456789][0123456789][0123456789][0123456789]'

   SET @MCspaces = '5[12345][0123456789][0123456789]
[0123456789][0123456789][0123456789][0123456789]
[0123456789][0123456789][0123456789][0123456789]
[0123456789][0123456789][0123456789][0123456789]'

   SET @DISCspaces = '6011 [0123456789][0123456789][0123456789][0123456789]
[0123456789][0123456789][0123456789][0123456789]
[0123456789][0123456789][0123456789][0123456789]'

   SET @AMEXspaces = '3[47][0123456789][0123456789]
[0123456789][0123456789][0123456789][0123456789][0123456789][0123456789]
[0123456789][0123456789][0123456789][0123456789][0123456789]'

   SET @DINNERSspaces = '3[068][0123456789][0123456789]
[0123456789][0123456789][0123456789][0123456789][0123456789][0123456789]
[0123456789][0123456789][0123456789][0123456789]'


   SET  @TableName = ''


   WHILE @TableName IS NOT NULL

   BEGIN

          SET @ColName = ''

          SET @TableName =

          (

                SELECT MIN(QUOTENAME(TABLE_SCHEMA) + '.' +
QUOTENAME(TABLE_NAME))

                FROM   INFORMATION_SCHEMA.TABLES

                WHERE         TABLE_TYPE = 'BASE TABLE'

                      AND    QUOTENAME(TABLE_SCHEMA) + '.' +
QUOTENAME(TABLE_NAME) > @TableName

                      AND    OBJECTPROPERTY(
```

Continued

```
                                        OBJECT_ID(
                                                QUOTENAME(TABLE_SCHEMA) + '.'
+ QUOTENAME(TABLE_NAME)
                                                 ), 'IsMSShipped'
                                              ) = 0
            )

            WHILE (@TableName IS NOT NULL) AND (@ColName IS NOT NULL)
            BEGIN
                  SET @ColName =
                  (
                        SELECT MIN(QUOTENAME(COLUMN_NAME))
                        FROM   INFORMATION_SCHEMA.COLUMNS
                        WHERE          TABLE_SCHEMA  = PARSENAME(@TableName,
2)
                               AND     TABLE_NAME    = PARSENAME(@TableName,
1)
                               AND     DATA_TYPE IN ('char', 'varchar',
'nchar', 'nvarchar')
                               AND     QUOTENAME(COLUMN_NAME) > @ColName
                  )

                  IF @ColName IS NOT NULL
                  BEGIN
                        INSERT INTO #CCRes
                        EXEC
                        (
                               'SELECT ''' + @TableName + '.' + @ColName +
''', LEFT(' + @ColName + ', 3630)
                               FROM ' + @TableName + ' (NOLOCK) ' +
                               ' WHERE ' + @ColName + ' LIKE ''' +
@VISANoExtras + ''' OR ' + @ColName + ' LIKE ''' + @MCNoExtras  + ''' OR ' +
@ColName + ' LIKE ''' + @DISCNoExtras + ''' OR ' + @ColName + ' LIKE ''' +
@AMEXNoExtras + ''' OR ' + @ColName + ' LIKE ''' + @DINNERSNoExtras + '''
                               OR ' + @ColName + ' LIKE ''' + @VISAdashes +
''' OR ' + @ColName + ' LIKE ''' + @MCdashes + ''' OR ' + @ColName + ' LIKE
''' + @DISCdashes + ''' OR ' + @ColName + ' LIKE ''' + @AMEXdashes + ''' OR
' + @ColName + ' LIKE ''' + @DINNERSdashes + '''
                               OR ' + @ColName + ' LIKE ''' + @VISAspaces +
''' OR ' + @ColName + ' LIKE ''' + @MCspaces + ''' OR ' + @ColName + ' LIKE
```

Continued

```
''' + @DISCspaces + ''' OR ' + @ColName + ' LIKE ''' + @AMEXspaces + ''' OR
' + @ColName + ' LIKE ''' + @DINNERSspaces + ''''
                          )
                END
            END
    END

    SELECT ColName, ColValue FROM #CCRes
END
GO
```

3.3 Policy Checks

Your policy must require that any time the primary account number (PAN) is displayed it must be masked, except when there's a specific need for the entire number. A maximum of either the first 6 or last 4 digits can be displayed.

3.3 Hands-on Assessments

Obtain samples of various locations where the credit card number appears, and verify that only the truncated number is shown unless the full number needs to specifically be shown. This includes account numbers shown on Web pages, invoices, transaction receipts, and so forth.

3.4 Policy Checks

Your policy must require that the PAN is at least rendered unreadable anywhere it is stored using a strong one-way hash, truncation, index token and pad, or strong encryption. If you are using disk encryption instead of file or column level database encryption, verify that your policy requires that the encryption process must not be tied to the operating system's access control mechanisms. Also verify that your policy requires that cardholder data stored for wireless networks is encrypted or sanitized there.

3.4 Hands-on Assessments

Take a sample of systems and verify that any time a PAN is stored, it is at least rendered unreadable using a strong one-way hash, truncation, index token and pad, or

strong encryption (such as 128-bit Triple-Data Encryption Standard [DES] or 256-bit Advanced Encryption Standard [AES]). Take a sample of data from database servers to verify that account numbers are not being stored in the clear. Sample removable media (e.g., backups) and audit logs to verify unencrypted account numbers are not being stored. Also take a sample of data coming from wireless networks to verify that it is encrypted when stored.

If you are using disk encryption, verify that the logical access to files is implemented using a mechanism separate from one included with your native file system. Sample systems to verify that the encryption keys are not stored on a local system. They should instead be stored on a floppy disk, CD-ROM, or other removable media and should be physically stored in a secure location. Take a sample of removable media that contain credit card account numbers and verify that account numbers are encrypted on the media.

3.5 Policy Checks

Verify that you have an updated policy that covers secure storage of encryption keys that would prevent their disclosure and misuse. Verify that the policy specifies that there are very few custodians. The policy should specify appropriate forms and locations for storing keys (keys should be stored in the fewest locations possible).

3.5 Hands-on Assessments

Verify that encryption keys are stored securely and are protected against disclosure and misuse. Also verify that key custodian assignments are up-to-date and access is restricted to only a few key custodians. Examine critical systems and verify that keys are stored separately from data in a secure location that only the key custodians have access to.

3.6 Policy Checks

Verify that the key management process is up-to-date and contains the following items.

- If you are a service provider and you share keys with customers for transmission of cardholder data, your policy must require that you provide documentation to your customers that describes how to securely store keys.
- Strong keys must be generated and used.
- Keys must be securely distributed and stored.

- Keys must be periodically changed; this must happen at least once a year.
- Old keys must be securely destroyed.
- Split knowledge and dual control of keys (keys where two or three key custodians have parts of a key and all are needed to reconstruct it) is used for keys that encrypt sensitive data.
- Procedures should prevent keys from being replaced without authorization.
- Keys that have been compromised or are suspected to be comprised must be replaced.
- Old or invalid keys must be revocated (e.g., with Rivest, Shamir, & Adleman [RSA] keys).
- Key management custodians must sign a form showing they understand their responsibilities.

3.6 Hands-on Assessments

Take a sample of critical systems and verify that you are currently generating and using strong keys. You can interview key custodians to verify that the keys are being securely distributed and securely stored. Find out when the last time was when the keys were changed and verify that this complies with the policy. Verify that keys are being securely destroyed. You can also interview key custodians to verify that keys are being split into two or three pieces for critical information. Also verify that over time the key sections have not all been given to one custodian. Verify that procedures are in place and working that prevent unauthorized substitution of keys. Verify that personnel responsible are familiar with and have followed policies to replace keys that have been compromised or are suspected to have been compromised. Also verify that those responsible are aware of and are following procedures for revocation old and invalid keys (e.g., RSA keys). Obtain copies of forms signed by key custodians that verify they understand and accept key-custodian responsibilities.

Requirement 4

Requirement 4 works to verify that you keep confidential data secure while it's traveling over networks.

4.1 Policy Checks

Verify that there is an up-to-date policy in place that contains the following items:

- Require that strong cryptography and secure protocols (such as SSL, TLS, or Internet Protocol Security [IPSEC]) be used to ensure secure transmission of cardholder data.
- Require that wireless networks use WPA, WPA2, IPSEC, VPN or SSL/TLS. WEP cannot be used by itself to protect confidential data on the network.
- Require that if WEP is being used, there is a minimum of 104-bit encryption key with a 24-bit initialization value and that it is only used in conjunction with WPA or WPA2, VPN, SSL, or TLS. Your policy should also require that WEP keys are rotated at least quarterly and automatically if your systems support this. Your access points must also restrict access based on Media Access Control (MAC) addresses.

4.1 Hands-on Assessments

Take a sample of your network devices and systems and verify that they are using strong encryption such as SSL, TLS, or IPSEC for transmission of confidential data. For example, for SSL or TLS Web pages, you should take a sample of pages that should be secure and verify that HTTPS appears in the Uniform Resource Locator (URL). You can also take a sample of transactions as they are received to verify they are encrypted (this can be done using a network sniffer such as Wireshark). Review the configuration of your systems to verify that only trusted SSL and TLS keys and certificates are accepted. When reviewing the configuration, you should verify that proper encryption strength is being used.

Anytime a wireless network is carrying cardholder data it should be encrypted. Verify that WPA or WPA2 is used whenever possible. You can also use IPSEC, VPN, SSL, or TLS instead of, or in conjunction with, WPA or WPA2. If WEP is being used, sample access point configurations to verify that a minimum of a 104-bit encryption key and a 24-bit initialization value is being used. Also, if WEP is being used, it should be in conjunction with WPA, WPA2, VPN, SSL, or TLS. Verify that access points are configured so that shared WEP keys are rotated at least quarterly or automatically if your system is capable of this. Also, by looking at a sample of access point configurations, verify that access is restricted based on MAC addresses.

4.2 Policy Checks

Verify that a policy is in place that requires that e-mail is always encrypted when it contains credit card account numbers. Unencrypted credit card data should never be sent over e-mail.

4.2 Hands-on Assessments

If you are sending PANs over e-mail, verify that your system is correctly configured to strongly encrypt these e-mails. You may also want to obtain a sample of e-mails and verify that credit card numbers are not being sent in the clear. Also interview employees to verify that they are following the company policy.

Requirement 5

Requirement 5 mandates that antivirus is on the systems and is up-to-date.

5.1 Policy Checks

Your policy must require that all computers have anti-virus software running on them that is capable of protecting against viruses and other types of malicious software, including spyware.

5.1 Hands-on Assessments

Take a sample of critical servers and wireless access points and verify the anti-virus software is installed. Verify that anti-virus software is capable of detecting, protecting against, and removing viruses and other types of malicious software, including spyware.

5.2 Policy Checks

Your policy must require that anti-virus software is up-to-date, running at all times, and capable of logging its activities.

5.2 Hands-on Assessments

Take a sample of systems, critical servers, and wireless access points and verify that anti-virus software is up-to-date, currently running, and generating audit logs. Verify that the master install has automatic updates and periodic scans enabled. Also verify that logs are being retained in accordance with your company's policy for log retention.

Requirement 6

Requirements 6 is used to verify that you develop and maintain secure systems and applications. This ensures you have the most recent patches installed and that you are using secure methods for developing software.

6.1 Policy Checks

An up-to-date policy must be in place that requires that all systems are patched with vendor-supplied patches within 30 days of a patch being released.

6.1 Hands-on Assessment

Take a sample of several different types of systems (critical servers, wireless access points, and so forth) and verify that they have all software patches installed on them. A software patch must never be out for more than 30 days without being installed on your systems. You may also use a tools such as Nessus or Microsoft Baseline Security Analyzer to help find systems that are missing patches.

6.2 Policy Checks

Verify that a policy is in place that outlines a method for receiving notifications about newly discovered security vulnerabilities.

6.2 Hands-on Assessment

Verify that your company is receiving news about the latest vulnerabilities that pertain to your systems. For example, you should be subscribed to an alert service that will send notifications about newly discovered problems. Several such services are freely available on the Internet. Interview employees responsible for securing systems to verify that they are receiving these alerts and are using the information to identify and mitigate new vulnerabilities.

6.3 Policy Checks

Examine your written software development processes to verify that it includes the following items:

- Software must be developed using an industry standard security development lifecycle.
- All changes, including patch, must be tested before the product is deployed.

- The test and development environment must be separate from the production environment.
- There must be separation of duties between personnel assigned to develop and test software and those assigned to the production environment.
- Live account numbers must never be used in development, or they must be sanitized before they are used.
- Test data and accounts must be removed before it is put on production systems.
- Custom application accounts, usernames, and passwords must be removed before applications become active or are released.
- Custom code must be reviewed to identify coding vulnerabilities prior to being put into production or being released to customers.

6.3 Hands-on Assessment

Interview developers to verify that the chosen security development lifecycle is being followed and is working to find and remove vulnerable code. Also verify with those responsible that all changes are tested before they are put into production. Interview employees to verify that testing and development environments are separate from production environments and that there is a separation of duties for personnel assigned to test/development and production environments.

Verify that live account numbers are never used in testing and development, or that they are sanitized before they are used. Take a sample of production systems to verify test data and accounts have been removed before putting a system into production. Verify in the sample that custom application accounts, usernames, and passwords are removed before software is made active or released to customers.

You should also interview employees to verify that an individual or team other than the code author reviews code for security problems before new code is put into production or changes are made to current code.

NOTE

Currently, code audits can be done by an internal individual or team, but as of June 30, 2008, this will change (Requirement 6.6 has more details on this).

6.4 Policy Checks

Verify that change control procedures are in place for security patches and software modifications that include the following items;

- Require that there is documentation of customer impact for any change made.
- Appropriate management personnel must sign-off on any changes.
- Operational testing must be performed for any changes.
- A back-out procedure must be in place for any changes.

6.4 Hands-on Assessment

Examine the three most recent software modifications or security patches for a sample of critical system components, and trace verify that the correct procedures were followed. For example, verify that customer impact was documented. Obtain management sign-off forms to verify that the correct management personnel signed off the change before it was done. Interview those who are responsible for testing and verify it was done for the most recent changes. Verify that back-out procedures are documented for each sample change.

6.5 Policy Checks

Verify that your software development process is up-to-date that requires all software is developed using industry-accepted secure coding guidelines such as Open Web Application Security Project (OWASP). It should specifically outline procedures to help secure Web applications against the following common vulnerabilities:

- Invalidated input
- Broken access controls
- Broken authentication and session management
- XSS
- Buffer overflows
- SQL injection or other injection flaws
- Error handling flaws
- Insecure storage

- Denial of service
- Insecure configuration management

6.5 Hands-on Assessment

Interview developers to verify they are using techniques to protect against vulnerabilities outlined in your software development process as described above. Verify with your testing team that these vulnerabilities are being tested for. Verify that programmers are being educated on secure programming techniques.

6.6 Policy Checks

Verify that your company has a policy that requires the use of a Web Application Firewall (WAF) and/or a code review of all custom Web application code. Also verify that code is re-evaluated after corrections are made.

6.6 Hands-on Assessment

Verify that a WAF is in place or that an outside group that specializes in auditing code for security vulnerabilities is performing regular security audits periodically and whenever there is a large change in the code base. If you're using a WAF, inspect its configuration to ensure that it is updated regularly.

Requirement 7

Requirement 7 ensures that only those who need to know sensitive information are given access to it.

7.1 Policy Checks

Verify that your policy is up-to-date that mandates that only personnel whose job requires that they have access to sensitive data are given access to sensitive data. Your policy must require that management signs a form that authorizes any personnel access to sensitive data.

7.1 Hands-on Assessment

Periodically obtain a sample of management sign-off forms and compare them to the access controls on associated systems, to verify that no more access is given than what is specified on the form.

7.2 Policy Checks

Your policy must require that systems with multiple users are set with default deny-all access to cardholder data, then specifically give access only to users who need access to the information.

7.2 Hands-on Assessment

Take a sample of critical systems and verify that they are set to deny-all access by default, and then only allow those that specifically need access to the information to perform their job. Verify the access controls set are still consistent with user's current jobs.

WARNING

Often, people get promoted, demoted, or simply shifted to another position and end up accumulating new privileges every time they move positions. Verify that this is not happening in your organization.

Requirement 8

Requirement 8 verifies that unique identification is being used to access systems and that only authorized people can perform operations.

8.1 Policy Checks

A policy must be in place that requires all users to have unique user IDs.

8.1 Hands-on Assessment

Take a sample of user IDs and verify everyone is using a unique username to access systems that contain sensitive data. Depending on the scale of your network, sometimes you can check logs to verify that all logins for a certain ID come from that user's computer. If you find exceptions (especially if there are a lot of exceptions), you may need to confront that person to see why the logins are taking place elsewhere. If they've shared their login information with another user, then proper steps should be taken to educate the user and fix the problem so it doesn't continue to happen.

8.2 Policy Checks

A policy should be in place that prohibits accounts that only need a user ID to log in. A password, token device, or biometrics must be required to log into any account.

8.2 Hands-on Assessment

Take a sample of critical systems on your network and verify that they are configured to require a username and a password, token device, or biometrics to authenticate users. You may also watch a sample of employees log into critical systems to verify one of the above methods is used in conjunction with their username.

8.3 Policy Checks

A policy must be in place that mandates that two-factor is required for remote access to networks. Technologies such as RADIUS or TACACS with a token, or VPN with individual certificates should be used.

8.3 Hands-on Assessment

Inspect system configurations to verify that technologies that require two-factor authentication are used. Verify that technologies such as Remote Authentication Dial-In User Server (RADIUS) or Terminal Access Controller Access Control System (TACACS) with a token, or a VPN with individual certificates are used. You can also take a sample of employees and ask them to login as if they were logging in remotely, and verify they're required to use two-factor authentication.

8.4 Policy Checks

A policy must be in place that requires that all passwords on all systems are encrypted when they're stored or transmitted

8.4 Hands-on Assessment

Take a sample of your system components (including network devices, wireless access points, and critical systems) and verify that passwords are encrypted when stored and transmitted. Most systems by default will only store passwords encrypted. For example, misconfigured Cisco routers can store passwords in the clear. If you are a service provider, take a sample of password files to verify that customer passwords are encrypted.

8.5 Policy Checks

Verify that password polices are in place for non-customer users and administrators that includes the following items:

- Policies must be in place to control addition, deletion, and modification of user IDs.
- Outline a process for verifying a user's identity when resetting their password, especially if they've requested the reset over the phone, e-mail, or other non-face-to-face method.
- Require that first time passwords for new users are not the same.
- Access for terminated employees is removed promptly.
- There are no accounts on the systems that have been inactive for over 90 days.
- Vendor accounts used for remote maintenance must only be active when they are in use.
- All employees that have access to cardholder data must be educated on password policies.
- Group, shared, or generic passwords and accounts cannot be used.
- Passwords must be changed at least every 90 days.
- Passwords must be at least 7 characters long and use both alphabetic and numeric characters.
- Not allow users to reuse any of their pervious four passwords.
- Require that an account is locked after six or more failed login attempts, and remain locked out for 30 minutes or until the administrator unlocks the account.
- Require that sessions that are idle for 15 minutes require the user to re-enter their password.
- Authentication procedures must be in place for all access to databases containing cardholder data.

8.5 Hands-on Assessment

You should have authorization forms for user accounts. Obtain these and verify that the access users are given on systems matches with what the form says they should have. Verify that only administrators have access to administrative consoles on wireless networks. Interview system administrators to verify that they are following company procedures to verify the identity of users when password resets are requested by e-mail, Web, over the phone, or other method that's not face-to-face. You could test this by choosing a sample of employees and have them request a password reset and verify the correct procedure is followed.

You can interview system administrators to verify that unique first-time passwords are given to new users. You could also test this periodically by using the normal procedure to request two fake new users (use the same procedure that's in place to set up new users including having management sign a form). Compare the passwords these users have been given to verify they're not the same, and then promptly have these accounts removed from the system.

You also need to verify terminated employees have their access revoked. To verify this, obtain a list of all employees terminated over the last 6 months and check a sample of these accounts to verify they have been terminated. Inspect systems to verify that there are no accounts on the system that have been inactive for more than 90 days. Also take a sample of vendor accounts used for maintenance and verify they're only active if they are currently being used.

Interview a sample of users to verify that they understand password policies and that periodic review of policies is taking place. This education can include things such as how to choose a good password, how to get a new password when needed, and how to protect your password (e.g., no post-its with your password and don't ever give it to anyone under any circumstances).

Take a sample of systems and determine that generic accounts (such as guest) are not enabled. You may also want to review system logs to verify that group and generic accounts are not being used. Review the password policy with system administrators to verify they understand it. As part of this, you should verify that administrators never give out shared accounts even when requested.

Verify that critical servers, system components, and wireless access points require that passwords are changed every 90 days by inspecting the configuration settings on a sample of systems. You can also obtain log files for a sample of systems to find when the last change was made. Verify that the settings for these systems require passwords

that are at least 7 characters long with both numeric and alphabetic characters, and that it keeps a history of past passwords and doesn't allow the user to re-use any of their previous four passwords. Also verify that systems are configured so that after six failed login attempts to an account then that account is locked. A simple way to test this is to use a known account, try to login more than six times, and confirm that the account is locked. The account should stay locked for 30 minutes or until the administrator unlocks it. You may also login to an account and wait for 15 minutes to verify it requires you to login again and check this setting on the servers. You also need to check database servers that contain credit card data and verify they require authentication for any user or application to use it. Also verify that only administrators are allowed to execute SQL queries on the server.

Requirement 9

Requirement 9 verifies that physical security is working. To test this one you will likely have to get up from your desk and do some walking.

9.1 Policy Checks

Verify that a policy is in place that mandates critical systems be physically secured using locks, cameras, and so forth. Also verify that your policy requires that backup tapes are stored for at least three months and that network jacks and network equipment are adequately protected.

9.1 Hands-on Assessment

Verify that badge readers, locks, and other physical security measures are being used to secure systems that store credit card data. One way to test this is to look on your network map and pick a sample of systems and go to the system administrator over that system and have them take you to that system. Verify that cameras are installed and running that monitor traffic into and out of these areas. To verify that tapes are being kept for at least three months, approach the employee that is responsible for archiving tapes and ask for tapes from three months ago.

You also need to verify that publicly accessible jacks are physically protected. For example, conference rooms with network jacks in them should be locked when not in use. Also, measures such as disallowing DHCP in conference rooms would help deter malicious users from using these jacks. Alternatively, if your policy requires it, you can verify that people are escorted at all times when they're in areas with live

network jacks. You also need to verify that wireless access points, gateways, and handheld devices are physically secured (e.g., locked in a closet).

9.2 Policy Checks

A policy must be in place that outlines assigning badges to visitors and precautions that should be taken to protect your environment from malicious visitors.

9.2 Hands-on Assessment

To verify that the policy is being followed, you can observer a contractor or a visitor entering your organization and verify that they get a badge and that it's easy to distinguish them from employees. Depending on the company you work for, you may even want to invite a friend to visit and verify that they are given a badge. You can also interview employees responsible for badges to verify they understand the policy. You should also periodically educate all users on actions to take if a visitor or someone without a badge is found wandering around your organization.

9.3 Policy Checks

Policies must require that visitors need authorization before entering areas where cardholder data is processed. Also, visitors must be given badges or other physical token that makes them easy to distinguish from employees. Visitor tokens or badges must expire and they must be asked to surrendered them when the visitor exits.

9.3 Hands-on Assessment

Interview employees to verify that authorization is required to enter areas where cardholder data is processed. Verify that employees know what to do if an unauthorized visitor attempts to enter a sensitive area in the company. Compare an employees badge to a visitor's badge or token to verify that they are different enough to make them easy to distinguish from an employee's badge. Observe visitors as they leave, to verify that they are asked to surrender their badge.

9.4 Policy Checks

A policy that requires a visitor's log be kept for at least three months for all visitors that enter your organization, unless this is restricted by law.

9.4 Hands-on Assessment

Ask for a copy of the visitors log and verify it's being used. You can also invite someone to visit you at work and verify later that his or her name appears in the log. Request copies of logs from three months ago to verify that visitor's logs are kept for at least three months.

9.5 Policy Checks

Policies must require that off-site backups are in a physically secure and fireproof location.

9.5 Hands-on Assessment

Periodically, visit the site where your media is stored to verify that it is stored in a secure and fireproof location.

9.6 Policy Checks

Policies must mandate that controls are in place for securing paper and electronic media in computer rooms and data centers. This would include items such as receipts, reports, faxes, computers, network systems, CDs, and disks.

9.6 Hands-on Assessment

Visit locations in your organization that should be securely storing paper and electronic media, and verify that the media is being stored in accordance with your company policy. This would also make a great subject for a review class with employees who work with cardholder data.

9.7 Policy Checks

Policies must require that media containing cardholder data be marked confidential. Also, when backups are taken off-site, they must use a secure carrier or other method that can be tracked.

9.7 Hands-on Assessment

Take a sample of media containing cardholder data and verify it is marked "confidential." Obtain the log that shows any media that is taken off-site and verify it is logged and that it's being sent using a secured carrier or other method that can be tracked.

You can also interview employees to verify that correct processes are being followed for marking sensitive data and sending it off-site.

9.8 Policy Checks

Policies must require that management approve all media that is moved from secure areas.

9.8 Hands-on Assessment

Obtain a recent sample of off-site media tracking logs and verify they had management's authorization before being moved.

9.9 Policy Checks

Verify that a policy is in place that requires strict control over media that contains credit card data, and that an inventory log is kept.

9.9 Hands-on Assessment

Get a copy of the most recent inventory log to verify that logging and inventory is happening. Go through the log and verify that the media is being stored securely.

9.10 Policy Checks

Policies must require that all media containing cardholder data must be securely destroyed when it is no longer need for legal or business reasons. Hardcopies must be run through a cross-cut shredder, incinerated, or pulped. Electronic media must be purged, degaussed, shredded, or otherwise destroyed in such a way that it cannot be reconstructed.

9.10 Hands-on Assessment

Interview employees to verify that media is being destroyed correctly. Take a sample of devices such as shredders, incinerators, and so forth to verify they work properly. Also, examine containers for material that will be destroyed to verify it's locked (e.g., a "to-be-shredded" container). Verify that electronic media is being destroyed correctly using a method described in your policy. You should also periodically educate employees on proper procedures to destroy media.

Requirement 10

Requirement 10 is used to verify you are correctly monitoring and testing your networks.

10.1 Policy Checks

A processes must exist for linking all system component access to specific users.

10.1 Hands-on Assessment

Interview system administrators to verify that audit logs are enabled on all systems. You can also take a sample of critical systems, including wireless networks, and verify that audit trails are enabled.

10.2 Policy Checks

Your policy must mandate that audit logs contain enough information to reconstruct the following:

- All access to cardholder data
- Actions taken by administrative privileges must be logged
- Any access to audit logs must be reviewed
- Invalid login attempts
- Identification and authentication mechanism are used
- Initialization of audit logs is logged
- Creation and deletion of system level objects is logged

10.2 Hands-on Assessment

Take a sample of access logs and verify that audit logs contain enough information to reconstruct all of the information above.

10.3 Policy Checks

Your policy must mandate that the following are contained in audit trail entries for all system components:

- User identification
- Type of event

- Date and time stamp
- If it was a success or failure
- Where the event originated
- Name of effected system, component, or resource

10.3 Hands-on Assessment

Get a sample of audit trails from various system components and verify that they include all of the information required above.

10.4 Policy Checks

A policy must be in place that requires that all system clocks are synchronized.

10.4 Hands-on Assessment

Take a sample of various servers to verify their system times are synchronized. Check their settings to verify they're getting their time from internal Network Time Protocol (NTP) servers instead of external sources (the exception is your NTP server can be receiving updates externally). Also verify that the most recent NTP is being used. You also need to verify that systems are set up to only receive time updates from certain hosts (your internal NTP servers).

10.5 Policy Checks

A policy must require that audit trails are secured so they cannot be altered by any users by including the following items:

- Viewing audit logs must be limited to users who need them for job-related reasons.
- Audit trail files must be protected against unauthorized modifications.
- Audit trail files must be promptly backed up to a centralized server or other media that is difficult to alter.
- Logs from wireless networks must be copied to a log server on the internal Local Area Network (LAN).
- File integrity monitoring and change detection must be in place to verify that log data cannot be altered without alters being generated.

10.5 Hands-on Assessment

Take a sample of systems and verify that only individuals with job-related needs have access to the audit trail files. Verify that current audit trail files are protected using access controls, physical, and/or network segmentation. Verify that the audit trail is being backed up by checking system settings and obtaining backup copies. Periodically restore one of these backups to verify the backup system is working correctly. You also need to verify that integrity monitoring or change detection software is being used to monitor any changes in the access log (adding new events to the audit trail does not need to be logged).

10.6 Policy Checks

Verify that your log review policy is up-to-date and requires that logs are reviewed at least daily on any critical servers, and those that perform security functions such as intrusion detection systems, authorization server, and accounting protocol servers. This daily review can be done using log parsing and alerting tools.

10.6 Hands-on Assessment

Interview employees responsible for daily log reviews to verify they are happening and exceptions are being followed up on. For example, you may want to ask them what events happened that day.

10.7 Policy Checks

Your policy must require that at least a years worth of audit trails be available online or on tape.

10.7 Hands-on Assessment

Take a sample of critical systems and verify that you have at least a years worth of audit trails online or on tape.

Requirement 11

Requirement 11 mandates that you verify that regular security tests are being done on your system.

11. 1 Policy Checks

Your policy must require that security controls, limitations, and network connections be tested at least annually to verify that they are working correctly to identify and stop unauthorized access attempts. Wireless analyzers must be used at least quarterly to identify all wireless devices in use.

11.1 Hands-on Assessment

Interview personnel responsible for running periodic tests to verify controls used to stop unauthorized access attempts are being tested as prescribed in the security policy. You should also run Kismet, Netsumbler, or other wireless analyzer to identify all wireless devices on your network.

11.2 Policy Checks

Policies must require that internal and external network vulnerability scans be done at least quarterly or after any significant change in your network.

Tools & Traps…

Using Nessus

Tenable's Nessus is a great vulnerability assessment tool that's available from www.nessus.org. It can run thousands of tests against many different systems. Installing Nessus is fairly straightforward and the Web site has some great documentation on it.

When running a Nessus scan, there are a few things you'll want to watch out for. For example, Nessus has a safe checks option. Enabling this will cause Nessus to not run tests that are likely to crash systems. This also somewhat cripples Nessus, because without running these tests the results will be less accurate. You will have to determine what the best option is in your environment.

11.2 Hands-on Assessment

You will likely have an Approved Scanning Vendor (ASV) running external scans quarterly, but you need to run internal ones as well. There are many great commercial and free tools out there to help you do this. A free tool that does very well at

assessing network vulnerabilities is Nessus. You may also want to run your own external vulnerability scans to verify that the ASV's results are accurate.

11.3 Policy Checks

Policies must require that penetration tests must be performed at least annually and after any significant change in your network.

11.3 Hands-on Assessment

Verify that you have the results of the most recent annual penetration tests. Also verify that if there were any large changes to your network that a penetration test occurred and you have the results available. Verify that both network-layer and application-layer penetration tests are performed.

11.4 Policy Checks

Policies must be in place that require that Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) systems are installed, up-to-date and monitored.

11.4 Hands-on Assessment

Verify that your IDS/IPS systems are running and are up-to-date. Also verify that employees are monitoring them and that the alert system is working correctly by checking IDS/IPS configurations and interviewing employees responsible for monitoring them.

11.5 Policy Checks

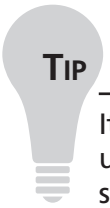
Policies must require that file integrity software is installed and monitored to detect changes in critical files.

11.5 Hands-on Assessment

Sample systems with critical files to verify that file integrity software is being used and is working correctly. Depending on your setup, you may want to test this by slightly modifying a protected file and verify an alert is sent.

Requirement 12

Requirement 12 is about maintaining your security policy and educating employees about these policies.



TIP

It will be much easier and your company will likely be more secure if you update your security policy often. That way you will be on top of new risks soon and it won't get so far behind that it becomes a mammoth task.

12.1 Policy Checks

Your security policy must be up-to-date and address all requirements in the PCI specification. Your policy must also include an annual process for identifying threats and vulnerabilities and perform a formal risk assessment. Your policy must also include a requirement to review the security policy itself at least once a year.

12.1 Hands-on Assessment

Review the policy to verify that it is being kept up-to-date and is being reviewed at least annually. Interview employees to verify that a formal risk assessment is occurring at least annually.

12.2 Policy Checks

Policies must require that daily operational security procedures are consistent with current PCI requirements.

12.2 Hands-on Assessment

Obtain a copy of security procedures and verify they are up-to-date with current PCI requirements. Also verify that your procedures are being followed by employees at your company.

12.3 Policy Checks

Verify that a policy exists for critical technology usage that defines proper use for all employees and contractors. This policy must include the following:

- Management must explicitly approve employee usage of critical technologies.
- Authentication must be in place to use critical technologies.
- A list must be maintained of all devices and personnel with access to critical technologies.
- All devices must be labeled with owner, contact information, and purpose.
- Requirements for acceptable locations on the network for critical technologies.
- A list must be maintained of all company-approved technologies.
- A requirement that requires that modem sessions are disconnected after a predefined period of inactivity.
- Modems for vendors must only be activated when they are needed by vendors, and deactivated immediately after use.
- Require that when cardholder data is accessed remotely via a modem, that it is prohibited to store cardholder data on a local hard drive, floppy disk, or other external media. It should also prohibit copy and paste and print functionality during remote access.

12.3 Hands-on Assessment

Interview management to verify that critical technologies are not being used without management approval. You can also obtain management sign-off forms to verify they are being used. Inspect configurations on a sample of critical systems to verify that authentication is in place to access these systems. Obtain the list of all devices and personnel authorized to use devices and verify that it is up-to-date. Sample network devices to verify they are labeled with owner, contact information, and purpose. Verify that the location of critical technology is in compliance with your security policy. Verify that products being used are on the list of company-approved products. Sample modems to verify they are configured to automatically disconnect after a predefined period of inactivity, and vendor modems are only activated when needed by vendors. Interview employees to verify that cardholder data is not being stored locally or on removable media, and that copy-and-paste and print functionally is prohibited during remote access.

12.4 Policy Checks

Verify that your policy is up-to-date that defines employee and contractor's security responsibilities.

12.4 Hands-on Assessment

Interview employees and contractors to verify that they understand their security responsibilities.

12.5 Policy Checks

Review that the following assignments are up-to-date in the security policy:

- Somebody is responsible for creating and distributing security policies and procedures.
- Somebody is formally assigned to monitor and analyze security events and distributing information to appropriate personnel.
- Somebody is formally assigned to create and distribute security incident response and escalation.
- Somebody is formally assigned to manage administrative accounts.
- Somebody is formally assigned monitor all access to data.

12.5 Hands-on Assessment

Interview employees to verify they understand and are following the polices as described above.

12.6 Policy Checks

Verify that your policy outlines a formal security awareness program to make all employees aware of the importance of cardholder data security. This should include educating employees when they are hired and at least annually. There must also be a requirement that mandates employees sign a form acknowledging they have read and understand the company's security policy and procedures.

12.6 Hands-on Assessment

Interview a sample of employees, some new and some older, and verify that they have been properly educated on the company's security policies and procedures. Also

verify that you have forms on file that show they have read and understand the procedure.

12.7 Policy Checks

A policy must be in place that requires that Human Resources perform background checks on new employees before they are hired.

12.7 Hands-on Assessment

Interview Human Resources to verify that background checks are happening.

12.8 Policy Checks

Verify that new contracts with service providers contain language that requires compliance with PCI standards that and that the third party is in charge of securing cardholder data.

12.8 Hands-on Assessment

Review a sample of contracts with third parties to verify that PCI compliance and securing cardholder data is part of the contract.

12.9 Policy Checks

Verify that your Incident Response Plan is up-to-date and that your policy requires that it's tested at least annually. Verify that you are aware of any new laws that you would need to comply with in the event of the compromise and that your incident response plan is updated accordingly. Also verify that your policy requires that personnel is available 24/7 to respond to alerts. It should require that employees are trained to know how to respond to security breaches. Your policy should also contain a requirement for intrusion detection and prevention and fire integrity monitoring.

12.9 Hands-on Assessment

Interview employees to verify that the plan is being well tested at least annually. Verify that you are researching new laws that would impact the requirements in your incident response plan. Also verify that there is somebody on alert 24/7 to respond to problems. Verify that your staff is being adequately trained on how to respond to a security breach. Also verify that intrusion detection and file integrity monitoring are in place and are being monitored.

12.10 Policy Checks

Verify that you have a policy in place for managing connections to processors and service providers that includes the following items:

- An up-to-date list of connected entities.
- Require that proper due diligence is happening before connecting to an entity.
- Require that any entity that you are connecting to is PCI compliant.
- Require that connecting and disconnecting follows and established process.

12.10 Hands-on Assessment

Obtain your list of connected entities and verify that it is up-to-date. Also interview employees to verify that due diligence is being performed prior to connecting to processors and service providers. Verify that as part of this check they verify that they are PCI compliant. Also interview employees to verify that processes for connecting and disconnecting to processors and service providers is being followed.

Summary

Security is fleeting. You've got it one minute and it's gone the next, but there are some steps that can be taken to keep yourself as secure as possible. Working with management and employees you can keep your company in a good position to combat many attacks now and in the future. Some very important parts to help keep you secure now and in the future is keeping your policy up-to-date, periodically assessing your security, and periodic training.

Solutions Fast Track

Security is a PROCESS, not an event

- ☑ You can't achieve security; it's a never ending process.
- ☑ You must constantly be assessing and working to mitigate risks.

Planning for periodic review and training, don't stop now

- ☑ You should plan now to train and review.
- ☑ Train your employees regularly to keep them reminded and up-to-date on company policies.
- ☑ Review the PCI requirements regularly to keep yourself up-to-date.

Performing a PCI Self Audit

- ☑ Regularly audit your systems to ensure they are still PCI compliant.
- ☑ Regularly review your policies to verify they are up-to-date and are working at your company.

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to **www.syngress.com/solutions** and click on the **"Ask the Author"** form.

Q: Can't I just buy some device that will make me secure?

A: No. There's no silver bullet out there that will magically make you secure. Security is a process, not an event or a piece of technology. You must be constantly keeping up with new risks and doing what you can to stop them on your network.

Q: Should I perform network scans even if I can't get management to sign off on it.

A: No way! You should never run any security tests on any system without permission from the owner.

Q: Can't I just run some scanners on my system and assume that I'm secure.

A: Many of these scanners work well but they're not 100 percent accurate and they definitely won't assess every problem. For example, untrained employees can cause huge security risks to your environment. While it's important to run these scans, it's also important to regularly check configurations and run other tests as well. It's also very important to be regularly educating your users.

Index

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W