



## **Penetration Hurts: Best Practices to Protect Sensitive Data and Achieve PCI Compliance**

*©2008 Rapid7 LLC All Rights Reserved*

# ***Penetration Hurts: Best Practices to Protect Sensitive Data and Achieve PCI Compliance***

---

Currently, the greatest threat on the Internet involves increased data theft, data leakage and targeted attacks for the purpose of stealing confidential information that can be used for financial gain. Acquiring unsecured financial information is the primary objective of hackers and organized crime in order to fuel a thriving black market for stolen credit card numbers, bank accounts, passwords, personal identification numbers and other data. These attacks affect more than just the online retailers. Breaches occur on point-of-sale, back office, and wireless technology systems.

## **COMPLIANCE IS A BUSINESS ISSUE**

According to the Privacy Rights Clearinghouse, at the end of April 2007, the total number of records containing sensitive personal information involved in security breaches was 154,525,715, involving companies that span all industries – retail, education, financial, government, telecommunications, healthcare, publishing, manufacturing – no industry is immune. All companies handle personal information of some type which subjects them to attack. Recently, the most successful attacks have been sophisticated, targeting particular organizations and designed for financial gain. Attacks have become more complex and involve other factors such as social engineering, insider abuse, and process breakdown in addition to technology weaknesses.

When personal data is lost, there is immediate anxiety and fear of having to deal with identity theft followed by a feeling of being violated. Individuals have to run credit checks and review them, put themselves on credit fraud watch lists, obtain new credit and debit cards, and possibly change where they bank. For someone going through this emotional time, they most likely will not be one of your biggest supporters.

## **Payment Card Industry Data Security Standard (PCI DSS)**

To combat data theft, the major credit card companies – Visa, MasterCard, American Express, Diner's Club, JCB, and Discover – have created a Data Security Standard that requires merchants, web-based retailers, and service providers that accept or process credit cards to comply with well-defined security directives. According to the standard, all members, merchants, and service providers that store or process credit cards must meet specific security requirements, which necessitate building a secure network and maintaining a vulnerability management program. To demonstrate compliance, merchants and service providers must provide security assessments and perform quarterly network scans to locate and fix vulnerabilities and reduce the risk of intrusion. Those organizations found not to be in compliance can face hefty penalties if data breaches are discovered.

PCI DSS is designed to facilitate global adoption of consistent data security measures to eliminate payment card fraud and clearly defines the steps needed to secure a networked environment. The scope of these requirements is broad but straightforward, giving direction to the service providers and merchants on what technologies, policies and procedures are needed to achieve compliance and incorporates best practices for perimeter security, data privacy, and application security.

Lacking any other guide to network security, the PCI DSS has been used by many network security professionals to develop a network security plan. But more specifically for any business that takes credit cards,

the PCI DSS is a framework of best practice requirements for those companies that handle sensitive credit card data to ensure that they properly protect that information. By banding together and supporting the PCI DSS, the major credit card companies have developed momentum for standard adoption.

Even though awareness is up by 90%<sup>1</sup>, industry statistics<sup>2</sup> indicate that more than 60% of merchants fail to meet the current standards and face the risk of stiff penalties imposed for non-compliance. According to Visa, penalties for noncompliance range from fines of up to \$500,000 to increased auditing requirements or even losing the ability to process credit card transactions. And these new regulations are holding all merchants regardless of size to much higher standards of performance when it comes to protecting the financial and personal information of their customers.

### What is PCI Compliance?

The PCI DSS requires that any merchant, processor, point-of-sale vendors, financial institutions and payment companies to implement processes, procedures and technology to protect credit card information. There are twelve PCI DSS-required controls that cover access management, network security, incident response, network monitoring and testing and information security policies.

Build and Maintain a Secure Network	<ul style="list-style-type: none"> <li>• Install and maintain a firewall configuration to protect data</li> <li>• Do not use vendor-supplied defaults for system passwords and other security parameters</li> </ul>
Protect Cardholder Data	<ul style="list-style-type: none"> <li>• Protect stored data</li> <li>• Encrypt transmission of cardholder data and sensitive information across public networks</li> </ul>
Maintain a Vulnerability Management Program	<ul style="list-style-type: none"> <li>• Use and regularly update antivirus software</li> <li>• Develop and maintain secure systems and applications</li> </ul>
Implement Strong Access Control Measures	<ul style="list-style-type: none"> <li>• Restrict access to data by business need-to-know</li> <li>• Assign a unique ID to each person with computer access</li> <li>• Restrict physical access to cardholder information</li> </ul>
Regularly Monitor and Test Networks	<ul style="list-style-type: none"> <li>• Track and monitor all access to network resources and cardholder data</li> <li>• Regularly test security systems and processes</li> </ul>
Maintain an Information Security Policy	<ul style="list-style-type: none"> <li>• Maintain a policy that addresses information security</li> </ul>

<sup>1</sup> According to Seanna Pitt, chairperson of the PCI Security Standards Council and vice president of merchant policy and data quality at American Express

<sup>2</sup> Presented by Visa at the Advanced PCI DSS Conference in New York in April 2007

For most merchants to comply with the PCI DSS standard and become certified, the process requires that you complete a detailed self-assessment questionnaire and receive quarterly network vulnerability scans for all Internet facing systems from an independent scanning vendor. For merchants that execute 6 million transactions annually or more, the regulations require a detailed onsite assessment. Merchants who process less than 20,000 transactions annually are still required to comply with the regulations, even though they are not currently required to be validated by the Card Associations. But regardless of your size, failure to comply can lead to steep penalties and unwanted publicity. In addition, merchants who do have an incident will automatically be treated as a level 1 merchant regardless of whether you qualify or not, requiring you to employ a Qualified Security Assessor to audit your environment. News of a security breach taints your brand, reduces consumer trust and results in serious fines and class action law suits from consumers or banks that had to reissue new credit cards.

## ***Benefits of Compliance***

Adhering to the PCI DSS standard shows that you are serious about protecting personal information which increases customer confidence in your business. Protecting sensitive information is no longer just about protecting credit card information. It has expanded into how businesses protect their key constituency -- customers.

The risks are too high to ignore the requirement to comply with the PCI DSS for all merchants. One breach can impact a business's financial status and reputation from which it may not be able to recover. By following the procedures of PCI DSS, organizations can effectively:

- **Protect customer personal data and increase customer confidence and trust** – Doing all you can to protect your customers' sensitive data sends a message that you care about your customers, building confidence and trust in your customer base.
- **Reduce the risk of financial losses** – Demonstrating compliance in the event of a breach can minimize the financial penalties. Avoiding a breach due to strong and consistent compliance to the standard will save you money over time.
- **Preserve their brand's reputation** – Brand is a significant company asset. Avoiding a security breach and adhering to the PCI DSS standard will protect your brand from the resulting damage to your reputation in the market.

## ***Security Best Practices Reduce Risk***

Policies, processes and training are as important to PCI compliance as any technologies you implement. Network and security administrators must be guided by policies that embed the security standard's requirements into ongoing operational activities

Developing a security best practices policy for your organization can help you put the controls in place to achieve PCI compliance. The plan covers processes that outline how you will develop and maintain security for your organization, technical controls that will be enforced to ensure that your data and infrastructure is secure, and consistently implementing the plan.

## **Where is the Data?**

Understanding where your credit card data is stored, where it moves through your network and processed and whether it is encrypted is an important first step in beginning to put together your PCI strategy and securing your data. It is common practices for employees to duplicate data in spreadsheets, documents and other unsecured files to share with others and simplify business processes, unknowingly exposing the company to violations.

Unnecessarily storing credit card data and failing to isolate the data from traveling across less secure parts of the network compounds the problem. Encryption is often inconsistent across a company's computer system and credit card data may be protected in some instances, but not others. You may not be aware of systems that have retained cardholder data such as data warehouses, staging servers, backup systems, desktops or other systems that for some reason received a copy of a transaction.

Retaining full magnetic stripe or CVV2 data is in violation of the PCI DSS requirements. The PCI standard only allows the account number, expiration date and name to be retained and cardholder data must never be stored on a server connected to the Internet. When asking for a CVV2 code, do not document or record it on any database after transaction authorization.

PCI compliance is more easily achieved by reducing the amount of cardholder data you store and reducing the number of systems that touch cardholder data. You may need to restructure your network to consolidate all systems that handle credit card transactions into a single network segment. By doing so, you reduce your risk of compromise, you simplify the management and execution of the compliance process, and you contain the scope of your PCI compliance validation efforts.

Companies using wireless networks to connect their remote locations to the central database for data consolidation either needs to encrypt the data for transfer or may want to consider moving to a more secure medium such as secure point-to-point virtual private network connections.

## **Vulnerability Scan – Your Best Friend**

Your networked environment is not static – new systems are introduced, laptops come in and out of the network, new software and upgrades get installed regularly. Regularly scanning your environment for software vulnerabilities and abnormal activity ensures you keep track of activity that could introduce new exposures. Scanning often ensures you uncover new exposures introduced by updates, new systems, new software or other changes to your environment.

If you have an online e-commerce application, ensure you guard against SQL injection attacks caused by insecure shopping carts. The credit card companies have created lists of validated applications that should be considered for use. Even if you use a proven shopping cart, ensure you scan your Internet facing systems for vulnerabilities that could compromise your online business.

## **Define and Enforce Security Policies**

To fulfill your responsibilities to those who entrust you with their personal information, developing a security policy that reduces your risk of exposing these individuals to the possibility of identity theft is essential. Defining a security policy for your organization begins with understanding the big picture of protecting sensitive information. It is a formal definition of what is allowed and what is not allowed, including acceptable use of

systems and data for all categories of users, including the administrators. Responsibilities need to be defined and employees need to understand how he or she contributes to the security of the organization.

Implementing industry defined security policies from Microsoft, NSA, the Center for Internet Security (CIS) and National Institute of Standards and Technology (NIST) is a good first step in ensuring your networks are properly secured.

The most critical policy is to ensure you know who is accessing what information and from where. Many merchants use generic usernames and passwords to access point-of-sale systems for simplicity but now need to replace them with user specific names and passwords so that you can monitor and manage access to your data.

### **Strong Reporting Capabilities a Must**

The easiest thing you can do to prove you are in compliance is to document your steps of protecting data. A frequently updated document that proves you have the best policies, practices and tools in place to maintain the confidentiality of your data will come in handy if your network is breached and data is stolen.

To ensure you have the information you need for your documented proof, ensure every security technology you implement comes with strong reporting capabilities. The reports delivered help your security staff understand the effectiveness of your program and whether you need to modify your policies. Robust reporting can help you identify instances where malicious hackers or anyone without authorization try to access credit card data. Installing products that centrally manage the IT assets and push out software patches and antivirus updates to the systems ensures all remote sites are up to date with security software. Being able to log and audit all transactions involving payment card data is required by PCI.

Detailed reports are also needed for meeting the needs of auditors ranging. Having tools that generate many types of reports - from your quarterly PCI scan reports to details on specific devices, vulnerabilities or other information – can help you show compliance if the auditors request this information.

### **Selecting Validated Payment Applications**

Any software vendor that develops applications for taking credit card payment should have their software validated by a third-party, Visa-accredited assessor as part of their development process. The card associations have developed a set of voluntary application best practices for software providers that ensure an acceptable level of security and reduce the scope and costs of compliance.

These best practices also pertain to custom applications you develop for your business:

- **Do not retain full magnetic strip or CVV2 data** – Ensure cardholder data is not recorded in any file or database including logs, diagnostic files, audit trails, transaction history, and images. If you must store cardholder information, you should never store it on a server connected to the Internet.
- **Protect stored data** – Mask any displayed cardholder data that you use to populate forms.
- **Provide secure passwords features** – Support unique usernames and complex passwords for all administrative access and access to cardholder data.
- **Log application activity** – Record and retain audit trails of anyone who accesses cardholder data.

- **Develop secure applications** – Implement system development practices, secure coding practices, code reviews and security testing; remove non-essential application accounts, usernames, and passwords, unnecessary and insecure services and protocols before applications go live.
- **Protect wireless transmissions** – Ensure you use strongly encrypted wireless connections deployed outside firewalls.
- **Test applications to address vulnerabilities** – Scan all applications, especially those running on Internet facing systems, before you deploy and regularly thereafter to ensure no exposures were introduced via upgrades or bug fixes.
- **Facilitate secure network implementation** – Remote access to your network needs to be secured via firewalls, VPNs, and two-factor authentication (username/password plus token). If the application transmits cardholder data, it must be encrypted, especially over public networks. All non-console administrative access must also be encrypted.

## ***Social Engineering – The Human Factor***

Social engineering is a term that describes the non-technical intrusion into your business environment that relies on human interaction, often involving tricking people in order to break normal security policies. Similar to traditional "con games" where one person is duped because they are naturally trusting, social engineers will use any technique to gain unauthorized information. Social engineering techniques include everything from phone calls with urgent requests to people with administrative privileges to viruses lurking behind email messages that attempt to lure the user into opening the attachments.

Most people have a tendency to trust someone initially and today's criminals know that. The naïve insider who falls for a phishing scam or takes a phone call from someone who needs 'inside' information occurs frequently in the workplace. Your employees need to be trained and tested periodically to ensure they understand the importance of compliance and are adhering to the security policies that describe these incidents and what they should information they should never give out over the phone. Training should include security policies and procedures on credit card acceptance and incident response.

To test your organization, call various organizations from a phone number without caller id and ask some simple questions to try and learn about your business from the employee on the phone. Does customer service want to be so helpful that they give out sensitive information on the phone such as passwords, account numbers or other information that help hackers gain access to your systems?

## ***Employing Outside Assistance***

Hiring security consultants that are experienced in holistically testing your organization's security is a valuable exercise. In a real consulting situation, Rapid7 consultants under contract to test network security used a combination of a case study, a helpful helpdesk resource and a SQL injection vulnerability to penetrate a customer account on a Web based portal. Alone, the penetration test and testing the human aspects of security are good, but used together the exposure became quite powerful. Eliminating the vulnerability and better training the helpdesk personnel on security policies would easily eliminate this situation but you need to know the issues are there in order to address them.

## ***Achieving PCI DSS Compliance***

Achieving PCI DSS compliance is no longer an option but a mandatory business requirement for any business that wants to maintain their customer relationships. Effective security policies that continuously assess and remediate enterprise systems keep your business compliant. By ensuring a continuous state of compliance, organizations can proactively eliminate threats which exploit the ever changing landscape of your network, ensure ongoing compliance and enjoy the peace of mind that a reliable, responsive and cost-effective IT infrastructure can offer.

## ***About NeXpose and Rapid7***

NeXpose Unified Vulnerability Management provides continuous, flexible protection from network security threats by accurately scanning Web applications, databases, network devices, operating systems and other software to find threats, assess their risk and create a remediation plan to enable quick resolution. Extensive and flexible reporting shows how certain vulnerabilities can effect an IT environment, helping security professionals prioritize the remediation effort, secure their networks and achieve compliance with government regulations, security configuration policies and the PCI Data Security Standard. NeXpose helps companies implement a measurable and proactive vulnerability management process to ensure a high level of network security without compromise. Rapid7 is a PCI Council Approved Scanning Vendor.

### **Rapid7 LLC**

Corporate Headquarters  
545 Boylston Street  
Boston, MA 02116

Phone: (617) 247.1717  
Fax: (617) 507-6488

West Coast Office  
898 N. Sepulveda Blvd.  
El Segundo, CA 90245

Phone: (310) 760-4640  
Fax: (310) 640-6885



© Copyright 2008 Rapid7 LLC. All rights reserved. Rapid7 and NeXpose are trademarks of Rapid7 LLC. All other brands and products are trademarks of their respective holders.