2016 SECURITYMETRICS GUIDE TO

PCI DSS COMPLIANCE

A RESOURCE FOR MERCHANTS TO BECOME COMPLIANT

securityMETRICS®

FOREWORD

Despite advances in security technology and regardless of increased government cyber security initiatives, attackers will not abandon their pursuit of unprotected payment card data.

Often, it's the small, simple, easy-to-correct things that go unnoticed, creating vulnerabilities leading to data compromise. In other cases, merchants with layers of sophisticated IT defenses are tripped up by an employee who opens an errant email or uses a less than complex administrative password.

The cultivation of a year-round PCI compliance and security culture is imperative to avoid these simple mistakes.

I hope the 2016 SecurityMetrics Guide to PCI DSS Compliance will help you better understand today's PCI trends and recommended best practices to protect data from inevitable future attacks.

GARY GLOVER
SECURITYMETRICS VICE PRESIDENT OF ASSESSMENTS
QSA | CISSP | CISA | PA-QSA

TABLE OF CONTENTS

2016 DATA BREACH PREDICTIONS

INTRODUCTION

When a merchant is suspected of experiencing a payment card data compromise, SecurityMetrics' Payment Card Industry Forensic Investigators (PFIs) are sent onsite to thoroughly analyze the point-of-sale (POS) or E-commerce environment, and help prevent the loss of payment card data.

Through a forensic examination of the in-scope computer systems related to the processing of customer payment card information, data acquired from the breach site can reveal when and how the breach occurred, contributing vulnerabilities, and aspects of the IT environment out of compliance with Payment Card Industry Data Security Standards (PCI DSS).

SecurityMetrics Forensic Investigators have witnessed the rise and fall of popular attack trends over 13 consecutive years. Here are three predictions for the future:

1. INSECURE REMOTE ACCESS WILL CONTINUE TO PLAGUE MERCHANTS

In a 2011 security alert Visa stated, "[i]nsecure remote access continues to be the most frequent attack method used by intruders to gain access to a merchant's point-of-sale environment." Not much changed in the ensuing five years.

This year—2016 will likely follow similar trends from the latter half of 2015, including insecure remote access as the largest single origin of compromise. If this intrusion technique worked in more than 29% of last year's investigated breaches, hackers will likely continue using that method until it is no longer effective.

Although Europay, MasterCard, and Visa (EMV) reduces the number of at-risk payment card accounts, it will not directly impact a hacker's ability to successfully gain access to a merchant's system through remote access. Unless an easier intrusion method presents itself in 2016, it is not likely breach trends in this arena will change.

* Disclaimer: SecurityMetrics PFIs are Qualified Security Assessors, but do not perform a complete QSA audit of each PCI requirement during a PCI forensic investigation. PCI DSS requirement data is analyzed to the extent observed during the course of an investigation.

2. LARGE-SCALE BREACHES WILL DECREASE, BUT HUMANS REMAIN HIGH-RISK

Due to increased EMV implementation in 2016, the frequency of large-scale breaches seen in 2015 headlines should begin to decrease. The decline will be slow at first, until more businesses implement EMV-enabled POS terminals and more issuers replace conventional magnetic stripe credit cards with EMV cards. The marriage of those two initiatives should contribute to a decline in the total number of compromised payment card accounts from card-present merchant environments.

However, when human beings are involved, no security solution is 100% secure. Employees inherently introduce the potential for inadvertent employee error. The point of vulnerability in a number of 2015's largest breaches was initiated by the action of a non-malicious person (usually an employee). The trend of employees leading businesses to compromise through simple actions will continue to occur as long as human beings are involved in the payment card process.

3. EMV IMPLEMENTATION INCREASES, WHILE E-COMMERCE ATTACKS INCREASE CHANGE

Attackers will find it increasingly difficult to obtain customer credit card account information from card-present environments, due to the increased prevalence of EMV technology throughout the United States. If U.S. EMV implementation follows the trends of Europe and Canada, we should see a marked decrease in successful attacks against card-present environments, followed by an increase of attacks against E-commerce targets.

The reality is, there are more than 8 million commercial businesses in the U.S., and most will require new EMV hardware. It is unreasonable to think that every merchant has implemented EMV technology. A shift in attacks should correlate to the percentage of EMV adoption.

While no environment will be perfectly secure in 2016, the push for EMV, updated PCI security standards, and improved security technology efforts will improve the landscape of payment card industry security.

WINDOW OF COMPROMISE

Nearly every business in America will experience system attacks from a variety of sources. Many merchants have systems, environments, software, or website weaknesses that can be exploited by attackers from the day their environment is set up. In other cases, a merchant becomes vulnerable because they fail to apply a security patch or make system modifications without properly updating related security protocols. Based on data collected in 2015 by SecurityMetrics Forensic Investigators, the average merchant was vulnerable for 1,133 days.

The window of compromise starts from the date an intruder accesses a business network and ends when the breach is contained by security remediation. On average, it took 833 days from the time a merchant was vulnerable for an attacker to compromise the system. Once compromised, attackers were able to capture cardholder data for an average of 123 days in 2015.

INCREASED WINDOW OF COMPROMISE

The 123 average days of card data compromise in 2015 may be attributed to aggregation methods employed by card data thieves.

Attackers have been known to save card data from malware scraping (or other tools), without using or selling the data for four to six months. (After six months, some payment card data begins expiring.)

Using this aggregation method prevents card brands from identifying malicious account activity too early, which would expose the data breach much sooner and greatly limit the amount of stolen credit card accounts attackers could acquire.

TOP 5 CATEGORIES OF FAILED VULNERABILITIES:

- SENSITIVE DATA EXPOSURE
- PLAINTEXT PASSWORD COMMUNICATION
- SECURITY MISCONFIGURATION
- EXPOSED DATABASE PORT
- CROSS-SITE SCRIPTING

IMPROVE PROCEDURES TO DECREASE THE WINDOW OF COMPROMISE

When an environment isn't actively monitored, breaches are more likely to go undetected for longer periods of time. The sooner a breach is detected, the less damage an attacker can do to a business. Your goal should be to create and practice the necessary procedures to protect data and warn of abnormal behavior in an environment.

From a forensic point of view, logs and audit trails are crucial to proving how, or if, an organization was compromised. Keeping track of critical actions (e.g., access to files, login attempts) can help identify key attack elements. Logs help track actions to an individual user and determine potentially suspicious activity. Assigning unique user identification also creates an atmosphere of accountability and can deter internal system abuse.

Once suspicious activity has been defined within an environment, intrusion detection/intrusion prevention systems (IDS/IPS) can be configured to notify of activity that might indicate an attack.

Change detection programs like file integrity monitoring (FIM) are especially useful for E-commerce environments because they track the original state of a file and report any changes, such as when an attacker hides malware within an otherwise legitimate file or application.

SECURITY TESTING

The two major types of vulnerability testing that should be performed in every merchant environment include penetration testing and vulnerability scans.

Penetration tests are an aggressive vulnerability testing approach in which analysts identify potential weaknesses and attempt to exploit vulnerabilities. For example, penetration testing is particularly helpful for companies developing their own applications, as it's important to have code and system function tested by an objective third party. This helps find vulnerabilities missed by developers.

Vulnerability scans are automated, affordable, high-level tests that identify certain weaknesses in network structures. Robust vulnerability scans can identify more than 50,000 unique external weaknesses. In addition to locating and reporting vulnerabilities, typical vulnerability scans also encourage a recurring and reliable process for repairing discovered problems. After a scan completes, it's necessary to repair located vulnerabilities and rescan to confirm that vulnerabilities have been addressed.

SECURITY POLICY AND EMPLOYEE TRAINING

Having clearly written policies and communicating those continuously to employees is really a critical part of having a secure environment. If management pushes a security culture through company policies, it gives the "why" that guides employees decisions. If there is no "why," people may fail to correctly implement controls and practices, or may implement them sporadically and leave gaps in security.

One pitfall, even in the most protected environment, involves the introduction of malicious content by human error. Activities as simple as employee email access or unauthorized Internet browsing can allow paths to and from untrusted networks.

Employees often inadvertently introduce malware into merchant systems by simply opening email attachments, downloads, or USB drives. They are often unaware of the threat they just allowed into the system. Creating, instructing on, and enforcing a sound security policy is the best way to secure an environment from employee error that could negate the effectiveness of previously established security policies.

RISK ASSESSMENT AND MANAGEMENT: VULNERABILITY VS. EXPLOITABILITY

A formal risk assessment should occur at least annually and after any significant network changes to identify threats and vulnerabilities. Risk assessments help avoid breaches by keeping you up-to-date with current trends, technologies, and threats. They also provide direction on next-step compliance efforts.

Addressing vulnerabilities in particular, decreases the time an attacker can compromise the system (i.e., window of compromise). Vulnerability management plans, which identify antivirus software, patch management, coding, and control changes, are particularly helpful. Plans help identify, classify, remediate, and lessen future instances of vulnerabilities. Creating a vulnerability management plan is central to decreasing the window of compromise.

A RISK ASSESSMENT SHOULD OCCUR AT LEAST ANNUALLY AND AFTER ANY SIGNIFICANT NETWORK CHANGES TO IDENTIFY THREATS AND VULNERABILITIES.

However, just because a system is vulnerable doesn't mean it's exploitable or likely to be exploited. Some vulnerabilities may require such a large number of preconditions that the chance of a successful attack is virtually absent. According to PCI Requirement 6, identifying the differing levels of exploitability should help an organization prioritize its actions to enhance IT security based on each identified vulnerability's perceived threat and risk level.

TAKEAWAYS

SecurityMetrics Forensic Investigators discovered some merchants previously knew of vulnerabilities that led to a breach. These organizations did not place sufficient priority to enhance their IT security and correct identified weaknesses. In the end, these merchants paid for the cost of a mandated forensic investigation, fines from their bank, fees from credit card issuers, and other costs to bring their IT security up to par. Their failure to initially correct the weak link in their system cost them quite a bit more than if they had practiced proactive remediation.

EARLY DETECTION AND CONTINUAL PROTECTION

Carefully track and manage an environment's actions to ensure early detection of a breach. Monitoring has the potential to decrease the window of compromise and thereby mitigate damage caused to an environment.

Maintain detailed logs that can be tracked back to individual users to help identify suspicious activity. Regularly review the logs and configure IDS/IPS as well as FIM to help keep watch over the environment.

Perform security testing on environments to identify weaknesses. Develop well-crafted IT security policies, ensure all employees are aware of their responsibilities with respect to the security policy, and practice a process to address security vulnerabilities by order of importance.

MALWARE TRENDS

TYPES OF MALWARE

Malware is commonly used to capture payment account information. Such malware is usually designed to target one of two common payment environments: POS or E-commerce. After analyzing collected data, 76% of 2015 investigations were in card-present environments (i.e., POS) and 19% of investigations took place in E-commerce environments.

POS MALWARE

Once hackers gain access to a POS system, they're likely to install malware. According to SecurityMetrics data, 78% of compromised POS merchants had malware on their systems, and in the last two years, Symantec identified POS malware has compromised 100 million payment cards and potentially affected up to one in three people in the U.S.

The most common type of POS malware is a memory scraper, designed to capture, or 'scrape' sensitive information from system memory (RAM) and return it to the attacker.

Malware found on merchant systems in POS environments during SecurityMetrics forensic investigations:

- Memory scraper
- Keylogger
- Trojan application

POS MEMORY SCRAPERS INCREASING IN POPULARITY

Although POS memory scrapers were first reported by Visa in 2008, attacker use of POS malware (and subsequent strains) became extremely aggressive in 2014 and 2015. In 2014, SecurityMetrics encountered one of the most sophisticated memory scrapers of any investigation previously performed. This malware knew the precise location in memory from which it should surgically extract the card data, leaving behind little to no forensic evidence.

Over the last few years, attackers have discovered that modifying existing malware to capture payment card data requires less work and allows them to remain under antivirus radar. Even if the original malware is picked up by signature-based software, the anti-virus software may not recognize different strains. Some malware files are even programmed to modify themselves on set time intervals, allowing them to slip past antivirus software indefinitely.

A strong correlation was found when comparing malware and insecure remote access. In 2015, 50% of merchants who were breached through insecure remote access also had memory-scraping malware on their system.

FORENSIC INVESTIGATORS DISCOVERED THAT 33% OF MERCHANTS HAD MEMORY-SCRAPING MALWARE INSTALLED ON THEIR SYSTEM.

MALWARE SUITES

The installation of malware suites was also a very popular tactic in 2015. By using a suite of malware designed for different functions, an attacker could adequately search for (or parse), locate, and export payment card data through FTP, email, or web traffic in a streamlined process.

SAMPLE OF MALWARE FILE NAMES:

- rundll.exe
- msi.exe
- nt01.dat
- nt02.dat
- nthome.dat
- ISScheduler.exe
- Toolbar.exe
- API.dll
- Cwd.dll
- fcntl.dll
- File.dll
- IO.dll
- p2x588.dll
- POSIX.dll
- re.dll
- runsvc32.exe
- util.dll
- win32.dll
- mstsc.exe
- winlogon.exe
- winhelp.exe
- defrag.cmd
- defrags
- check.zip
- socks3-098.exe
- socks3-1498
- c4.exe

Keyloggers are commonly included in malware suites, but were much less popular in 2015. Keylogger malware secretly records every keystroke a user makes on a computer or mobile device, including USB credit card swipe devices. Using this method, the malware can easily collect typed information like passwords, bank account numbers, or credit cards typed on payment pages, as well as magnetic credit card stripe data. Luckily for merchants, antivirus products have become much better at detecting malicious keyloggers in the last few years.

E-COMMERCE MALWARE

E-commerce environments provide a completely different set of obstacles for organizations because most vulnerabilities are due to weaknesses in software or website coding. E-commerce malware usually manifests as code-based attacks used to obtain cardholder data.

Malware found on merchant systems in E-commerce environments during SecurityMetrics forensic investigations:

- Remote file inclusion
- SQL injection
- Malicious code

E-COMMERCE ATTACKS: REMOTE FILE INCLUSION

Remote file inclusion is accomplished when attackers embed malicious files into legitimate applications. This type of malware can typically be found by employing FIM software, which looks for changes in the original software, such as an increase in the original size of the application. In 2015, remote file inclusion was found in 33% of E-commerce merchant investigations.

E-COMMERCE ATTACKS: SQL INJECTION

After exploiting software vulnerabilities, SQL injection feeds information into web forms not coded to reject illegitimate characters. Attackers can gain information about a business database based on the web form output. If hackers receive enough information about a database, it's only a matter of time until they can ultimately gain administrative access. SQL injection was responsible for 25% of 2015's E-commerce merchant breaches.

E-COMMERCE ATTACKS: MALICIOUS CODE AND COMMAND SHELLS

Malicious code affected 25% of investigated E-commerce merchants. Malicious code and command shell attacks can vary depending on the weaknesses in written code of the environment under attack. In one instance, the original code was replaced by a modified code that would write captured data to a temporary file for later export.

TAKEAWAYS

IMPLEMENT NEW TECHNOLOGIES TO COMBAT MALWARE

One commonality discovered by investigators was the storage of malware in memory instead of on a hard drive, which reduces its detectability. Attackers are taking advantage of the milliseconds between card swipe and encryption by the payment application. They engineer malware to reside solely in memory, a place often hidden to antivirus applications.

However, end-to-end encryption solutions, like point-to-point encryption (P2PE), encrypt data at swipe and maintain encryption until the moment of authentication, preventing attackers from accessing payment card data in memory. Merchants are encouraged to implement a P2PE solution to decrease the likelihood of falling victim to memory-scraping or similar malware that relies on capturing card data before or while unencrypted.

A P2PE PROCESS ENCRYPTS YOUR DATA, WHICH WILL KEEP IT SAFE FROM ATTACKERS.

PROACTIVELY UPDATE AND REPORT

SecurityMetrics and other security companies routinely provide samples of newly discovered malware iterations to antivirus and anti-malware firms so they can update their malware signatures on a regular basis. It is essential to frequently update your antivirus/anti-malware programs to ensure protection against known malware.

Merchants can also use outside sources, such as US-CERT, SANS, and vendor antivirus threat feeds to help them identify newly discovered malware. They can then review their logs for new threats or configure IDS/IPS systems to alert and report on suspicious activity that may indicate malware installation.

SECURE E-COMMERCE ENVIRONMENTS

Common antivirus applications aren't always properly configured, updated, or adept at detecting malware in an E-commerce environment. Implementing FIM to examine files for unauthorized modifications can help further protect an E-commerce environment. FIM checks the integrity of operating systems and application software files by comparing current file contents to a trusted master list, and triggers notifications when unauthorized changes are detected.

PCI DSS COMPLIANCE TRENDS

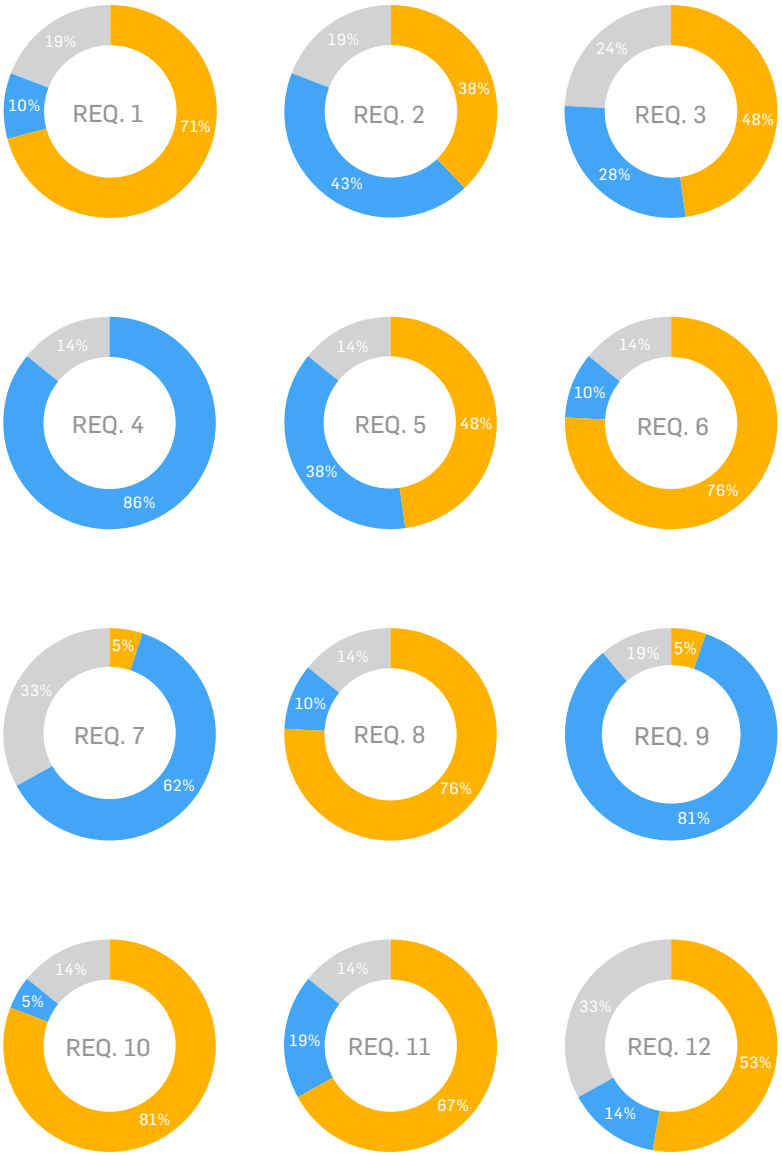
PAYMENT SECURITY

The Payment Card Industry Data Security Standard (PCI DSS) was established in 2006 by the major card brands (Visa, MasterCard, American Express, Discover Financial Services, and JCB International). All businesses that process, store, or transmit payment card data are required to implement the security standard to prevent cardholder data theft. The investigation of numerous credit card data compromises has confirmed that the security controls and processes required in the PCI DSS are essential to protecting cardholder data.

Merchants often have a difficult time attaining (or maintaining) compliance for a variety of reasons. Many smaller merchants believe it's too technical or costly, while others simply don't believe it's effective and refuse to comply. In fact, our data concluded that the average merchant, at the time of data compromise, was not compliant with at least 47% of the PCI DSS requirements.

ON AVERAGE, CUSTOMERS GO TO SUPPORT 2.5 TIMES BEFORE BECOMING COMPLIANT.

WERE PCI REQUIREMENTS IMPLEMENTED AT TIME OF COMPROMISE?



These graphs discuss each requirement and their subsequent implementation by compromised merchants in 2015.

NO

PARTLY YES

INFORMATION NOT AVAILABLE

MOST FREQUENTLY IMPLEMENTED REQUIREMENTS

The following requirements had the highest implementation rates in 2015:

- **PCI DSS Requirement 4- Encrypt transmission of cardholder data across open, public networks:** The reason implementation of Requirement 4 is so high is not because of great implementation processes, rather that most current payment applications automatically encrypt cardholder data once it reaches the application itself.
- **PCI DSS Requirement 7- Restrict access to cardholder data by business need to know:** The more a business unnecessarily exposes sensitive data to those employees and others who don't need access, the more likely they are to suffer a breach.
- **PCI DSS Requirement 9- Restrict physical access to cardholder data:** Very few (if any) of the 2015 data breaches involved a data thief physically present at the breached location.

LEAST IMPLEMENTED REQUIREMENTS

Of the requirements that contributed to breaches, the following requirements had the lowest implementation rates in 2015:

- **PCI DSS Requirement 1- Install and maintain a firewall configuration to protect cardholder data:** Non-compliance with this requirement includes both the absence of a firewall altogether, as well as a poorly configured firewall.
- **PCI DSS Requirement 6- Develop and maintain secure systems and applications:** This commonly applies to E-commerce merchants that develop in-house payment applications without ensuring their security.
- **PCI DSS Requirement 8- Identify and authenticate access to system components:** The most common areas where merchants are found non-compliant with Requirement 8 are a failure to assign unique credentials to all system users and failure to implement multi-factor remote access authentication.
- **PCI DSS Requirement 10- Track and monitor all access to network resources and cardholder data:** Very few merchants track or monitor access to cardholder networks through logs and log monitoring.
- **PCI DSS Requirement 11- Regularly test security systems and processes:** A lack of testing security controls and processes contributed in 29% of breaches.

TOP 10 FAILING SELF-ASSESSMENT QUESTIONNAIRE SECTIONS

We scanned our merchant database in search of the top 10 areas where merchants struggle to become compliant. These are the results:

1. **Requirement 12.5.3—12.6.a:** Establish, document, and distribute security incident response and escalation procedures, administer user accounts, and monitor/control access to data.
2. **Requirement 12.10.1.a:** Verify incident response plan responsibilities, business recovery procedures, data backup processes, and legal requirements for reporting compromises.
3. **Requirement 9.9.2.b:** Verify personnel are aware of procedures for inspecting devices and that devices are periodically inspected for evidence of tampering.
4. **Requirement 12.1:** Establish, publish, maintain, and disseminate a security policy.
5. **Requirement 1.1.3.a:** Establish a current diagram that shows all cardholder data flows across systems and networks.
6. **Requirement 9.9.2.a:** Verify documented processes include procedures for inspecting devices and frequency of inspections.
7. **Requirement 12.3.3:** List devices and personnel with access to data.
8. **Requirement 12.3.5:** List acceptable uses of used technology.
9. **Requirement 1.2.1.b:** Examine firewall and router configurations to verify inbound and outbound traffic is limited to that which is necessary for the cardholder data environment.
10. **Requirement 1.1.3.b:** Ensure a process exists to keep the cardholder diagram current.

TAKEAWAYS

Unfortunately, 2015 showed some significant decreases in compliance levels when compared to 2014. None of the investigated breached merchants in 2015 were found to be compliant with PCI DSS. Furthermore, in nearly every case, the vulnerabilities attackers leveraged to gain access to merchant systems were covered by specific sections of the PCI DSS. In other words, had the merchant been compliant with those sections of the PCI DSS, the breach likely would not have occurred.

PCI DSS: WHAT YOU NEED TO KNOW

PCI DSS 3.2 (and supporting documents) was released on April 28, 2016. On October 31, 2016, PCI DSS 3.1 will retire, and at this time all assessments wll need to use version 3.2. Until January 31, 2018, the new requirements introduced will be considered best practice and become requirements starting February 1, 2018.

1. SECURE SENSITIVE DATA

Security clearances aren't just for government officials or high-tech organizations. For example, restricting access to the administrative portions of POS systems or hotel management applications can lower the chance of malware entering a system.

RESTRICT ACCESS TO CUSTOMER DATA ON A NEED-TO-KNOW BASIS.

PCI DSS 3.2 delves into employee restrictions to safeguard access to customer data with a handful of new requirements:

- **Requirement 5.3** reminds us that antivirus shouldn't be altered without managerial approval. If just anyone can disable antivirus, the business might be vulnerable to malware slipping past the unguarded system.
- **Requirement 7.1.1** requires a role-based access control system. This means employee access to card data and systems should only be granted on a need-to-know basis.
- **Requirement 9.3** is all about controlling physical access to sensitive areas. If an employee's job doesn't require them to have access, they shouldn't have access.

2. REVIEW AND REVISE PROCESSES

Many breaches are caused by lack of process review. Errors can easily occur due to ignorance, poor planning, lack of attention, or timing, and can lead to security decay.

The PCI Council believes double-checking software, processes, and devices is an important part of a secure business environment, and added these requirements:

- **Requirement 9.9.2** ensures merchants regularly examine POS devices to confirm they haven't been tampered with. This is especially important for POS systems left out in the open and unattended for a long period of time (such as gas station terminals).
- **Requirement 10.6.2** states the importance of reviewing logs of all system components. Periodically reviewing logs helps determine if suspicious activity is occurring.

3. KEEP THOROUGH DOCUMENTATION

Documentation is the failsafe that keeps your hands clean, keeps your company transparent, and keeps your security efforts organized.

That's probably why PCI has so many requirements about documentation:

- **Requirement 1.1.3** asks merchants to create a cardholder data flow diagram to show how cardholder data enters and flows through the network.
- **Requirement 2.4** requires a document that lists all in-scope devices and their function (e.g., POS systems, computers, mobile devices).
- **Requirement 9.9.1** is very similar to 2.4, and requires merchants to maintain an up-to-date list of all devices including physical location, serial numbers, and make/model.
- **Requirement 11.1.1** asks merchants to maintain a complete list of authorized wireless access points and justify why they are needed in the business environment.
- **Requirement 12.8.5** requests two lists: the PCI requirements your third-party service provider meets, and a list of PCI requirements your business is required to meet. These lists help avoid miscommunication between third parties and merchants by outlining who is responsible for certain PCI requirements. In a franchisee's case, it would probably be beneficial to have a similar list explaining the security responsibilities of both you and your franchisor.

4. SSL/TLS NO LONGER SECURE

PCI DSS 3.2 addresses the insecurity of Secure Sockets Layer (SSL) and some Transport Layer Security (TLS) encryption protocols.

Effective immediately, all SSL and early TLS versions are no longer considered strong cryptography. PCI DSS requirements directly affected are:

- **Requirement 2.2.3:** implement additional security features for any required services, protocols, or domains considered insecure.
- **Requirement 2.3:** encrypt all non-console administrative access using strong cryptography.
- **Requirement 4.1:** use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks.

Merchants already using systems and devices that utilize SSL and TLS must discontinue use of those systems and devices before June 30, 2018.

IF YOU USE SSL/TLS AND NEED TO CONTINUE USING THESE TOOLS:

First, remember not to add any new systems or technologies that use older versions of SSL/TLS. If you need to continue using SSL/TLS to continue regular business operations, the following examples explain your options:

- Upgrade to a current, secure version of TLS configured not to accept fallback to SSL or early TLS.
- Encrypt data with strong cryptography before sending over SSL/early TLS (for example, use field-level or application-level encryption to encrypt data prior to transmission).
- Set up a strongly-encrypted session first (e.g. IPsec tunnel), then send data over SSL within the secure tunnel.
- Check firewall configurations to see if SSL can be blocked.
- Check that all application and system patches are up-to-date.
- Check and monitor systems to identify suspicious activity indicating a security issue.

PCI DSS 3.2: KEY CHANGES OVERVIEW

PCI DSS 3.2 (and supporting documents) was released on April 28, 2016. On October 31, 2016, PCI DSS 3.1 will retire, and at this time all assessments wll need to use version 3.2. Until January 31, 2018, the new requirements introduced will be considered best practice and become requirements starting February 1, 2018.

Key changes in PCI DSS 3.2 include:

- Revised SSL and early TLS sunset dates as outlined in the Bulletin on Migrating from SSL and Early TLS
- Expansion of requirement 8.3 to include use of multi-factor authentication for administrators accessing the cardholder data environment
- Additional security validation steps for service providers and others, including the "Designated Entities Supplemental Validation" (DESV) criteria, which was previously a separate document.

UPDATED MIGRATION DATES

In December 2015, the migration dates for companies to move from SSL and early TLS to the latest version of TLS were moved up from June 2016 to June 2018. The PCI Council wanted to reflect that date change in the latest version of PCI DSS.

Many businesses are opting to stick to the old date so they don't have to deal with the extra exposure. Having SSL encryption is very risky to security since it has many exploitable vulnerabilities. So even though the deadline has been extended, it's a good idea to make those changes as soon as possible.

MULTI-FACTOR AUTHENTICATION REQUIRED IN AND OUT (8.3)

PCI DSS 3.2 will evaluate additional multi-factor authentication for administrators within a Cardholder Data Environment (CDE). Multi-factor authentication is an effective way to secure your CDE, and is a requirement under PCI DSS. To properly configure multi-factor authentication, you must have at least two of three things:

- Something you know (username, password, etc.)
- Something you have (getting a code from your phone)
- Something you are (Fingerprint and other biometrics)

Prior to PCI DSS 3.2, multi-factor authentication was just required for remote access to the network by employees, administrators, and third parties. But now, even if your connection is within the CDE, you need to do multi-factor authentication. As with all the PCI DSS requirements, this is a reflection of the current threat landscape. This change helps strengthen security within your CDE as well as outside it.

Additionally, make sure that you "incorporate multi-factor authentication for all remote network access (both user and administrator, and including third-party access for support or maintenance) originating from outside the entity's network."

INCORPORATING DESIGNATED ENTITIES SUPPLEMENTAL VALIDATION INTO PCI DSS

PCI 3.2 will incorporate some extra validation procedures in the Appendix. In addition to full PCI DSS validation, designated entities determined by Acquirers or Payment Brands must have some additional validation that determines whether a business's day-to-day practices are reflective of their compliance.

The additional validation procedures are for designated entities to ensure they are PCI compliant on a day-to-day basis.

An example would be looking at a list of all the change controls in a merchant's environment for the past year. These procedures could include anything that shows the day-to-day compliance.

CLARIFYING MASKING CRITERIA (3.3)

PCI DSS 3.2 clarifies masking criteria for primary account numbers (PAN) when displayed. Masking is described as hiding information from view; this is not the same as encryption. When displaying a credit card number or bank identification number (BIN), you are allowed to display, at a maximum, the first 6 and last 4 numbers. If you go beyond these requirements, you're not compliant.

Additionally, you need to have "a list of roles that need access to displays of more than the first six/last four (includes full PAN)."

Whether or not you should display less PAN numbers could depend on various legal requirements. Another note worthy item that relates, if your business stores PAN, you're also required to encrypt and properly secure it.

CHANGE MANAGEMENT PROCESS (6.4.6)

PCI DSS 3.2 explains that you need to have a change management process to ensure that all new or changed systems and networks implement all relevant PCI DSS requirements, upon completion of a significant change. Documentation should include these updates.

Examples of possible requirements that could be impacted:

- Network diagram is updated to reflect changes.
- Systems are configured per configuration standards, with all default passwords changed and unnecessary services disabled
- Systems are protected with required controls—e.g., file-integrity monitoring (FIM), anti-virus, patches, audit logging
- Sensitive authentication data (SAD) is not stored and all cardholder data (CHD) storage is documented and incorporated into data-retention policy and procedures
- New systems are included in the quarterly vulnerability scanning process

SERVICE PROVIDER WRITTEN AGREEMENT (12.8.2)

PCI DSS 3.2 has further explained that "the extent to which the service provider is responsible for the security of cardholder data will depend on the particular service and the agreement between the provider and assessed entity." You still need to maintain a list of all PCI requirements your service providers meets, and a list of PCI requirements they're required to meet.

NEW SERVICE PROVIDER REQUIREMENTS

PENETRATION TESTING REQUIREMENTS (11.3.4.1)

For service providers, if you use segmentation, perform penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods.

Validation of PCI DSS scope should be performed as frequently as possible to ensure PCI DSS scope remains up to date and aligned with changing business objectives.

CRYPTOGRAPHIC ARCHITECTURE (3.5.1)

Service providers need to interview responsible personnel and maintain a documented description of cryptographic architectures, including:

- Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date
- Description of the key usage for each key
- Inventory of any HSMs and other SCDs used for key management

TIMELY DETECTION AND REPORTING (10.8, 10.8.1)

Service providers are required to "examine detection and alerting processes and interview personnel to verify that processes are implemented for all security controls, and that failure of a critical security control results in the generation of an alert." Examples of critical security control systems include:

- Firewalls
- IDS/IPS
- FIM
- Anti-virus
- Physical access controls
- Logical access controls
- Audit logging mechanisms
- Segmentation controls (if used)

Service providers need to respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include:

- Restoring security functions
- Identifying and documenting the duration (date and time start to end) of the security failure
- Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause
- Identifying and addressing any security issues that arose during the failure
- Performing a risk assessment to determine whether further actions are required as a result of the security failure
- Implementing controls to prevent cause of failure from reoccurring
- Resuming monitoring of security controls

ESTABLISH RESPONSIBILITIES FOR PCI AND DATA (12.4.1)

Executive management needs to establish responsibility for the protection of cardholder data and a PCI DSS compliance program to include:

- Overall accountability for maintaining PCI DSS compliance
- Defining a charter for a PCI DSS compliance program and communication to executive management

QUARTERLY PERSONNEL REVIEWS (12.11, 12.11.1)

Service providers need to perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes:

- Daily log reviews
- Firewall rule-set reviews
- Applying configuration standards to new systems
- Responding to security alerts
- Change management processes

In addition, you need to maintain documentation of quarterly review process, including:

- Documenting results of the reviews
- Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program

WHAT IS REQUIRED OF YOUR ORGANIZATION?

PCI DSS 3.2 introduced several changes, particularly about extending PCI scope and the introduction of new Self-Assessment Questionnaire (SAQ) categories.

PCI scope deals with environment systems that must be tested and protected to become PCI compliant, while an SAQ is simply a validation tool for merchants and service providers to self-evaluate their PCI DSS compliance.

System components most likely in scope for your environment may include:

- Networking devices
- Servers
- Switches
- Routers
- Computing devices
- Applications

Basically, if the people/process/technology component stores, processes, or transmits cardholder data (or is connected to systems that do), it's considered in scope and must be protected.

Then, filling out a PCI SAQ is the best way to make sure you aren't missing any business security requirements. There are different SAQs a merchant must choose from, depending on the way you process, store, or handle credit and debit cards. For example, if you do not have a storefront and all your products are sold online through a third party, you probably qualify for SAQ A or SAQ A-EP. The different SAQ types will be further explained later in this section.

85% OF SECURITYMETRICS CUSTOMERS STARTED THEIR SAQ AND FINISHED.
84% OF SECURITYMETRICS CUSTOMERS STARTED THEIR SAQ AND ARE PASSING.

AN AUDITOR'S PERSPECTIVE

PCI SCOPING

To discover your own PCI scope and what must be included for your PCI compliance, you need to identify anything that processes, stores, or transmits cardholder data, can initiate a connection to any of the systems that handle cardholder data, and evaluate what people and systems are communicating to your systems. For instance, call centers usually overlook QA systems, which often store cardholder data in the form of call recordings.

Ask yourself:

- What do you do as an organization?
- How do you make money?
- Why do you handle card data?
- How do you store, process, or transmit this data?

There are always processes you might not realize. For example, if you're a retail store that swipes cards, do you ever take card numbers over the phone or receive emails with card information? Are any paper orders received? Many times organizations have finance, treasury, or risk groups that have post-transactions processes involving cardholder data. It is important to include these processes when determining scope.

Don't forget power outage procedures in which card data is manually taken down. In most call centers, agents aren't trained that card data should never be written. When the application they use for recording cardholder data freezes, they tend to resort to typing or writing it down in a temporary location and retrieving it later for entry. These temporary locations are rarely considered in an organization's PCI compliance efforts, but can lead to increased risk and need to be included in PCI scope.

Often, paper trails of hand-written information or photocopied payment card data can sometimes fill multiple rooms. Even if card data is 10 years old, it is still in PCI scope.

If you access a web page for data entry, there's a decent chance card data can be found in temporary browser cache files. In addition, it's the website developer's responsibility to make sure websites don't generate cookies or temporary log files with sensitive data. However, merchants don't always have full control of their website, which is why it's important to evaluate all systems for cardholder data, even where you don't expect it to reside.

You might think your databases are set up to encrypt all cardholder data. However, servers you consider out of scope will often hold temporary files, log files, or back-ups with tons of unencrypted data. System administrator folders on file servers are also common culprits, as they often

back up failing servers in a rush to prevent data loss without considering the PCI implications.

Don't panic if you do find data where it doesn't belong. Usually organizations can find ways to fix the process and delete this data rather than add servers to their scope. A simplified way to find unencrypted card data is by running a card discovery tool such as PANscan®.

For organizations with web portals, if someone mistypes card data into an address or phone number field, it is still considered in PCI scope. Organizations need to have methods to detect these mistakes and prevent or delete them. Some use a data loss prevention (DLP) solution to help them with this process.

The next step in determining your PCI scope is to find everything that can communicate with the devices you have identified. This is often the hardest part about scoping because you may not understand what can communicate to your systems.

Ask yourself:

- How do you manage your systems?
- How do you log in to them?
- How do you backup your systems?
- How do you connect to get reports?
- How do you reset passwords?

If you have a server that handles cardholder data, you must always consider what else talks to that server. Do you have a database server in some other zone you consider out of scope, but is reaching that web server to pull reports and save data? Anything that can initiate a connection to an in-scope server that handles cardholder data will be in scope for compliance. There are very few, if any, exceptions to this.

If you want to get your systems out of scope, make sure your defined in-scope servers are communicating outbound to specific destinations for data or services they need, rather than allowing other systems to have access to these in-scope servers.

– TREVOR HANSEN
QSA | CISSP | CDCDP

PCI 3.2 SAQ TYPES

SAQ	Description	# of Questions	Vulnerability Scan	Penetration Testing
A	E-commerce website (third party) • Fully outsourced card acceptance and processing • Merchant website provides an iframe or URL that redirects a consumer to a third-party payment processor • Merchant cannot impact the security of the payment transaction	22	N	N
A-EP	E-commerce website (direct post) • Merchant website accepts payment using direct post or transparent redirect service	191	Y	Y
B	Processes cards via: • Analog phone, fax, or stand-alone terminal • Cellular phone (voice), or stand-alone terminal • Knuckle buster/imprint machine	41	N	N
B-IP	Processes cards via: • Internet-based stand-alone terminal isolated from other devices on the network	82	Y	N
C-VT	Processes cards: • One at a time via keyboard into a virtual terminal • On an isolated network at one location • No swipe device	79	N	N
C	Payment application systems connected to the Internet: • Virtual terminal (Not C-VT eligible) • IP terminal (Not B-IP eligible) • Mobile device (smartphone/tablet) with a card processing application or swipe device • View or handle cardholder data via the Internet • POS with tokenization	160	Y	N
D	E-commerce website • Merchant website accepts payment and does not use a direct post or transparent redirect service Electronic storage of card data • POS system not utilizing tokenization or P2PE • Merchant stores card data electronically (email, e-fax, recorded calls, etc.)	329	Y	Y
P2PE	Point-to-point encryption • Validated PCI P2PE hardware payment terminal solution only • Merchant specifies they qualify for the P2PE questionnaire	33	N	N

Note: Entities using SSL/early TLS have 2 additional PCI DSS requirements in their SAQ.

AN AUDITOR'S PERSPECTIVE

PCI DSS CHALLENGES VARY BASED ON ORGANIZATION SIZE

From what I've seen, smaller companies are less likely to consistently follow established policies and procedures. Because they only have a handful of systems and very few personnel with administrative access to the systems, they don't see the benefit of following processes and procedures. Many of these institutions view change control and documented hardening standards as busywork. They often ask: "Why take time to document when you can spend time getting it done?"

Large enterprise organizations are usually good with documenting their policies and procedures. They normally have very specific and thorough change control processes, and always follow the documented approval process before implementation. Unfortunately due to their environment size and the different entities involved in management, their reaction time tends to be much slower, and contradictory decisions are often made by different stakeholders. When vulnerability scans or penetration tests identify weaknesses that may place the cardholder data environment (CDE) at risk to compromise, it's not always apparent which group should be responsible for addressing the vulnerability. Sometimes one stakeholder will make decisions that have unintended consequences in other areas of the CDE.

Across the board, organizations are not leveraging many of the PCI requirements in a way that actually increases security for their CDE. For instance, PCI requires that all systems send their logs, and that those logs are reviewed daily. PCI also requires change detection or FIM on CDE systems to detect unauthorized changes to key files and directories. To achieve compliance, organizations will set up log monitoring and FIM, but then ignore every alert coming their way. They may technically have FIM and log monitoring in place, but these systems are not making their environments any more secure. If organizations do not take the time to tune these systems to reduce everyday noise and set up processes to respond to genuine alerts, the only thing they gain are SAQ checkmarks.

The same goes for a number of security controls. Very few organizations are fully leveraging technologies and practices required by the PCI DSS to improve and secure their environment. They use this technology to "check the PCI compliance box". Organizations are often more concerned about being PCI compliant than secure.

For large organizations, an internal employee should take charge of PCI compliance. Additionally, they must have a self-auditing process to ensure security practices are properly in place throughout the year. PCI compliance should not be about an annual PCI audit.

For smaller organizations, at the bare minimum, set-up a PCI email user or active directory account for PCI and add reminders in the calendar to ensure security processes required to be performed throughout the year are not forgotten (e.g., quarterly vulnerability assessment scans, semi-annual firewall reviews, etc.). Evidence collected when completing these tasks can then be sent to that PCI account for storage. This is a low or no-cost solution that can help key personnel keep PCI DSS compliance on their minds throughout the year, and will help document evidence they need to provide for their self-assessment (or to their assessor) during annual review.

For larger organizations with a change control ticketing system, establish tickets for all of the quarterly, semiannual, and annual tasks and assign them to the appropriate employees to ensure tasks are performed. Evidence from these tasks can then be saved within the ticket. Often the technical and business departments will need to work together to complete these tasks.

In many large enterprise environments the business operations side is responsible for requesting openings in the firewalls and providing business justification, and a technical team is in charge of implementing that change. In these environments semiannual firewall reviews are not usually very successful if performed by only one team. The business operations team usually doesn't have the technical expertise to read and understand firewall configurations, and the technical team may not know if a rule is still needed for the business to function. Getting both teams to participate will ensure a more successful firewall review.

– MIKE SIMPSON
QSA

REQUIREMENT 1:

PROTECT WITH FIREWALLS

FIREWALL CONFIGURATION

A common mistake regarding firewalls is assuming they are a 'plug and play' technology. After initial installation, additional effort is almost always required to restrict access and protect the CDE.

The end goal of firewall implementation is to filter potentially harmful Internet traffic from the Internet and other untrusted networks to protect valuable confidential data. In E-commerce applications, a firewall can also be used to limit traffic to only essential services needed for a functioning CDE. By identifying sensitive systems and isolating them through the proper use of a firewall (network segmentation), merchants can more precisely control what type of access is allowed into and out of these zones, and more easily protect valued data.

HARDWARE FIREWALL VS. SOFTWARE FIREWALL

Secure payment card environments rely on both hardware and software firewalls. A hardware firewall is typically installed at the perimeter of an organization's network to protect internal systems from the Internet. Hardware firewalls are also used inside the environment to create isolated network segments separating the CDE from non-CDE systems. PCI also requires a firewall be placed between systems that store cardholder data and all other systems, even internal ones. Software firewalls are used to protect a single host, particularly mobile devices that can move "outside" of the secure corporate environment.

HARDWARE FIREWALL	
PROS	CONS
Most robust security option	Generally more expensive
Protects an entire network	Difficult to configure properly
Can segment internal parts of a network	

SOFTWARE FIREWALL	
PROS	CONS
Better facilitates mobile workers outside the corporate network	Doesn't protect an entire network
Less expensive	Fewer security options
Easier to maintain	Cannot be used as the sole perimeter defense in a PCI DSS compliant environment

FIREWALLS AREN'T FAIL-SAFES

Having a firewall in place did not stop attackers from finding vulnerabilities through remote access applications. In fact, 83% of merchants breached through insecure remote access had a firewall in place. Of those, 33% had a firewall configuration that met PCI DSS requirements.

CORRECTLY CONFIGURE FIREWALLS

Firewall configuration is crucial to prevent attacks. The technology must be configured to accurately allow access to ports/services. Firewalls should be configured to filter both inbound and outbound traffic. If an attacker does happen to get into a system, outbound firewall rules can make it more difficult to export stolen data.

Firewalls should also be used to implement segmentation within an organization's network. When merchants create a secure payment zone firewalled off from the rest of the day-to-day business traffic, they can better ensure their CDE only communicates with known and trusted sources, and it limits the size of the CDE and potentially lowers scope.

Further, initial intrusion in many of 2015's investigated data breaches began in areas of the merchant's network that shouldn't have given the attacker access to the CDE. For example, since the merchant's network was configured as a "flat network" (i.e., the entire network is protected only by a perimeter firewall, with no internal segmentation) it was not difficult for the attacker to migrate from the point of entry (e.g., employee laptop or work station) to the card data or other sensitive systems.

IN 2015, ONLY 24% OF INVESTIGATED MERCHANTS HAD PROPERLY CONFIGURED FIREWALLS. 90% OF THE MERCHANTS WHO WERE NON-COMPLIANT WITH PCI DSS REQUIREMENT 1 COULD HAVE REACHED COMPLIANCE WITH REQUIREMENT 1 IF THEY HAD PROPERLY CONFIGURED THE FIREWALL ALREADY IN PLACE.

AN AUDITOR'S PERSPECTIVE

REQUIREMENT 1: FIREWALL ARCHITECTURE

Large environments typically have firewalls in place, at least at the perimeter of the network. Care needs to be taken to select firewalls that support the necessary configuration options to protect critical systems and provide segmentation between the CDE and other internal and external networks.

Smaller merchants sometimes struggle to understand firewalls, and may not have the necessary in-house expertise to configure and manage them correctly and securely. If this is the case, a PCI-validate third party service provider should be contracted to provide assistance, rather than simply deploying a default configuration and hoping for the best.

It may seem obvious, but leave as few holes as possible in your firewall. Rules should be as specific as possible for your environment. Spend the time to identify specific destinations, don't just allow all access to the Internet. Along the same line, if you have third parties that remotely support your environment, limit that inbound access to specific sources.

Firewalls are a first line of defense, and attention needs to be given to the logs and alerts they generate. Often, the volume of log data can be overwhelming, so merchants turn them off or discard them altogether. It's important (and required) to review firewall logs daily, in order to identify patterns and activity that indicate attempts to breach security. There are many good software packages available to help merchants deal with the volume of log data and to more easily pick out the important data that requires you to take action.

For Requirement 1, remember three things:

1. Strict firewall rules
2. Pay attention to what logs tell you
3. Review firewall configurations frequently and adjust as necessary

– DAVID PAGE
QSA | CISSP

IT CHECKLIST

IMPLEMENT FIREWALLS

THINGS YOU WILL NEED TO HAVE:

- Firewall
- Limited traffic into Card Data Environment to that which is necessary (1.2.1a)
- "Deny All" rule for all other inbound and outbound traffic (1.2.1b)
- Stateful Inspection/Dynamic Packet Filtering (1.3.6)
- Documented business justification for each port or protocol allowed through the firewall

THINGS YOU WILL NEED TO DO:

- Position firewall to prohibit direct inbound and outbound traffic from Cardholder Data Environment (1.3, 1.3.3)
- Create secure zone for any card data storage, must be separate from DMZ
- Outbound connections from Cardholder Data Environment must be explicitly authorized (1.3.5)
- Document all firewall policies and procedures (1.2.1.a, 1.2.1.b, 1.2.3, 1.3, 1.3.3, 1.3.5, 1.3.6)

THINGS YOU MAY NEED TO DO:

- Install a firewall between wireless networks and Card Data Environment (wireless only) (1.2.3)

REQUIREMENT 2:

USE ADEQUATE CONFIGURATION STANDARDS

DEFAULT PASSWORD WEAKNESSES

Devices such as routers or POS systems come straight from the vendor with factory settings like default usernames and passwords. Defaults make device installation and support easier, but also mean every model originates with the same username and password. Default passwords are simple to guess, and most are even published on the Internet.

Merchants are often unaware that default settings are used in their environment. Data security weaknesses introduced to a merchant's system by third-party providers/vendors, such as IT support and POS vendors, are a rapidly growing concern. Merchants trust that the third-party provider will configure their systems securely. If the third-party provider fails to change default passwords and implement multi-factor remote access authentication, in the event of a data breach it's unfortunately the merchant that remains liable.

In one SecurityMetrics forensic investigation, it was discovered that a third-party IT vendor purposely left POS system default passwords in place to facilitate easier future system maintenance. Default passwords might make it easier for IT vendors to support a system without learning new passwords each time; however, convenience is never a valid reason to forego security, nor will it reduce liability.

Most default passwords and settings are well known throughout hacker communities and are found via a simple Internet search. When defaults aren't changed, it provides attackers an easy gateway into a system. Disabling vendor defaults on every system with exposure to a CDE protects against unauthorized users.

Passwords should be changed every 90 days, and contain at least 7 characters including numeric and alphabetic characters. Passwords that fall short of these criteria can usually be broken using a password-cracking tool.

SYSTEM HARDENING

Any system to be used in the CDE needs to be hardened before being put into production. The goal of hardening a system is to remove any unnecessary functionality and to configure what is left in a secure manner. Every application, service, driver, feature, and setting installed on a system introduce possible vulnerabilities.

According to PCI DSS, to comply with Requirement 2.2, merchants must **"**address all known security vulnerabilities and [be] consistent with industry-accepted system hardening standards." Some good examples of hardening guidelines are produced by the following organizations:

- Center for Internet Security (CIS)
- International Organization for Standardization (ISO)
- SysAdmin Audit Network Security (SANS) Institute
- National Institute of Standards Technology (NIST)

But merchants can use and research other resources as well, such as the following:

- Information Assurance Support Environment (IASE)
- VMware environments for hardening virtual systems

SYSTEM CONFIGURATION MANAGEMENT

Consistency is key when trying to maintain a secure environment. Once system hardening standards have been defined, it is critical that they are applied to all systems in the environment in a consistent fashion. Once each system or device in the environment has been appropriately configured, you still aren't done. Many organizations struggle to maintain standards over time, as new equipment or applications are introduced into the environment.

This is where it pays to maintain an up-to-date inventory of all types of devices, systems, and applications that are used in your CDE. However, the list is no good if it doesn't reflect reality. Make sure someone is responsible for keeping the inventory current and based on what is actually in use. This way, applications or systems that are not approved for use in the CDE can be discovered and addressed.

Many organizations, especially larger ones, turn to one of the many system management software packages on the market to assist in gathering and maintaining this inventory. These applications are able to scan and report on hardware and software used in a network and can also detect when new devices are brought online. These tools are often also able to "enforce" configuration and hardening options, alerting administrators when a system is not compliant with your internal standard.

AN AUDITOR'S PERSPECTIVE

REQUIREMENT 2: SYSTEM CONFIGURATION

You're required to use industry accepted configuration or hardening standards when setting up your servers, firewalls, or any system in-scope for PCI.

Examples of system hardening practices include disabling services and features you don't use, uninstalling applications you don't need, limiting systems to perform a single role, removing or disabling default accounts, and changing default passwords and other settings. Permitting anything unnecessary to remain on a system opens you up to additional risk and possible vulnerability.

The key to system configuration and hardening is consistency. Once you have documented a standard that meets the requirements of your environment, make sure processes are in place to follow the standard as time goes on. Keep your standard and process up-to-date to take into account changes to your business or requirements.

Automated tools can simplify the task of enforcing configuration standards, allowing administrators to quickly discover systems that are out of compliance.

– DAVID PAGE
QSA | CISSP

IT CHECKLIST

VENDOR DEFAULTS

THINGS YOU WILL NEED TO HAVE:

- A secure way to access and manage systems in your environment (2.3)
- An inventory of all hardware and software used in the CDE
- Documented configuration standards for all types of systems in the CDE

THINGS YOU WILL NEED TO DO:

- Assign a system administrator and/or knowledgeable personnel the responsibility of configuring system components (2.2.4)
- Implement a system hardening guide covering all components of the CDE (2.2.a)
- Disable and uninstall any unnecessary programs, services, guest accounts, scripts, drivers, features, subsystems, file systems, and web servers. Document which services and programs are allowed (2.2.2, 2.2.5)
- Change vendor-supplied default usernames and passwords. Remove or disable unnecessary default accounts before installing a system on the network (e.g., operating systems, security software, POS terminals, routers, firewalls, SNMP) (2.1.a, 2.1.b, 2.1.1.b, 2.1.1.c)
- Document security policies and operation procedures for managing vendor defaults and other security settings. Inventory all systems within scope of the payment application environment and keep inventory up-to-date (2.4, 2.5)

THINGS YOU MAY NEED TO DO:

- Use technologies such as VPN or TLS for web-based management and other non-console administrative access. Ensure all traffic is encrypted following current standards (2.3, 2.1.1.d)
- If wireless Internet is enabled in the CDE, change wireless default settings including encryption keys, passwords, and SNMP community strings (2.1.1)
- Enable only one primary function per server (e.g., logging server, web server, DNS) (2.2.1)

REQUIREMENT 3:

SECURE CARDHOLDER DATA

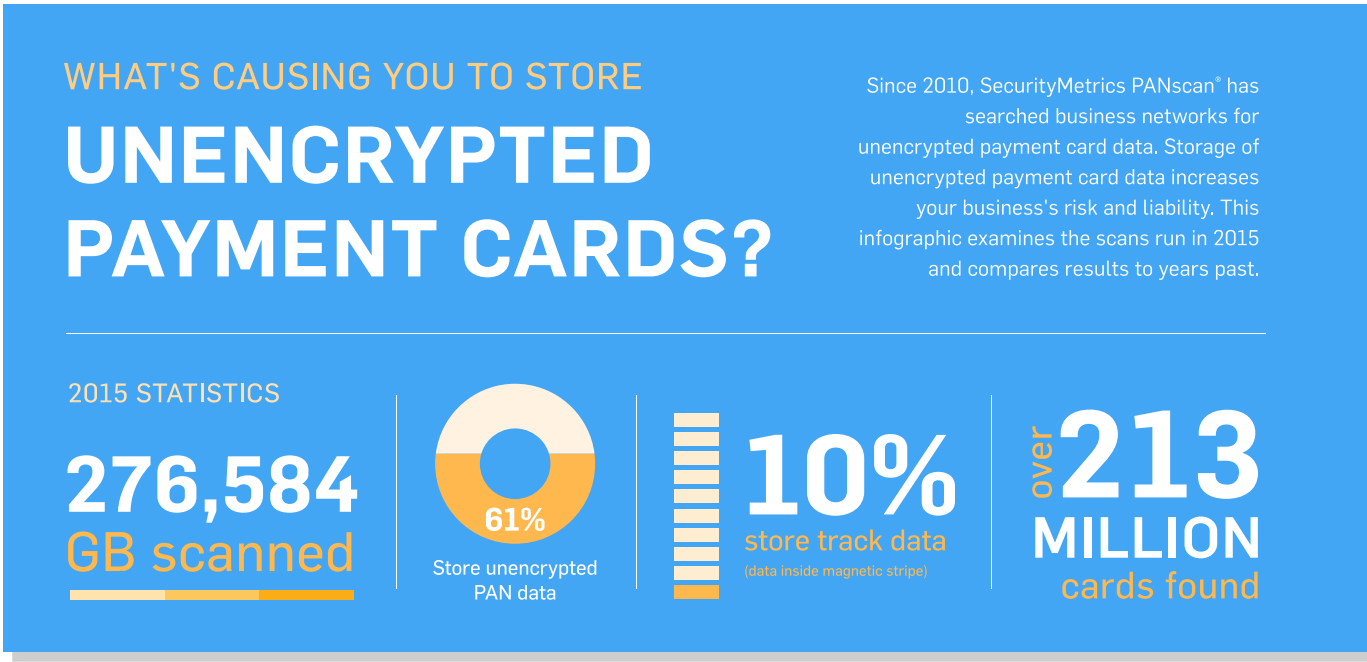
STORED CARD DATA

When cybercriminals hack a payment system, they cannot steal payment data that isn't there. That's why it's important to keep your system clean of insecurely stored card data. Unencrypted payment card data has a way of creeping in where you least expect it.

According to PCI DSS requirement 3, stored card data must be encrypted using industry-accepted algorithms (e.g., AES-256). The problem is many merchants don't know they store unencrypted Primary Account Numbers (PANs). In the latest study by SecurityMetrics, 61% of merchants were found to store unencrypted PANs.

Not only must card data be encrypted, the encryption keys must be protected as well. Not protecting the encryption key location using a solid PCI DSS encryption key management process is like storing your house key pushed into your front door lock.

Assign the responsibility of keeping unencrypted card data off your systems to an individual or team. Have this person/team define and follow a process of periodic data discovery cycles to recheck and ensure systems remain clean of unencrypted card information.



SOURCE HOW MUCH CREDIT CARD DATA ARE YOU STORING INFOGRAPHIC

FIND WHERE CARD DATA IS HELD

An essential part of eliminating stored card data is through the use of a valid card data discovery tool and methodology. Remember, payment card data can easily leak due to poor processes or misconfigured software. You must look where you ***think*** the data is, and then look where it ***shouldn't*** be.

PCI DSS 3.1 Requirement 1.1.3 requires a current cardholder flow diagram for all card data flows in your organization. A card data flow diagram is a graphical representation of how card data moves through an organization. As you define your environment, it's important to ask all organizations and departments if they receive cardholder information, and then define how their answers may change card data flows.

To accurately craft your card data flow diagram, ask yourself:

- What device(s) am I using for transactions? A virtual terminal? POS system?
- What happens to the card data after a transaction?
- When is data encrypted? Is it even encrypted at all?
- Do I store card data before it's sent to the processor for approval?
- How does settlement occur? Real time or end of day?
- How is data authorized and returned by the processor?
- Is card data backed up on my system? Are backups encrypted? Is my backup server at a different data location?
- Where might card data be going or moved in processes not part of authorization and settlement?

In addition, you should regularly run a cardholder data discovery tool (such as PANscan). These tools help identify the location of unencrypted PAN data. Knowing where PAN data is stored helps confirm whether or not your CDE is secure. It also helps identify which processes or flows might need to be fixed. Once you identify new processes, you can begin to determine how to either fix the process or add it into your normal environment flow.

	DATA ELEMENT	STORAGE PERMITTED	ENCRYPTION REQUIRED
Cardholder Data	Primary Account Number (PAN)	YES	YES
	Cardholder Name	YES	NO
	Service Code	YES	NO
	Expiration Date	YES	NO
Sensitive Authentication Data	Full Track Data	NO	Cannot Store per Req. 3.2
	CAV2/CVC2/CVV2/CID	NO	Cannot Store per Req. 3.2
	PIN/PIN Block	NO	Cannot Store per Req. 3.2

AN AUDITOR'S PERSPECTIVE

REQUIREMENT 3: PROTECTING CARDHOLDER DATA

Some of the biggest data issues organizations face are: having a data retention policy, understanding that policy, and following the policy.

IT security must work with the legal team and executives to decide what data the company holds onto, why they need it, and the length of time it's held. This communication often doesn't happen. Security staff will often draft data security policiesto meet PCI DSS compliance, but if it isn't adopted and enforced from the executives down, company processes will never change.

Policy enforcement must include requirements to encrypt data once received, timeframes to keep data, and a documented procedure to delete unnecessary payment card information that doesn't meet policy specifications.

Next, its imperative to understand what data you actually have. Map out all the flows to understand where data moves in your organization. For example, you may not know that the accounting department captures card data from a database and stores it in spreadsheets or that cardholder data is being saved in log files.

The best practice to find data is through a scanning program, **like PANscan**. Once all card data is found, make sure you consult your policies and PCI DSS to determine what you're allowed to keep. For example, PCI DSS prohibits track data storage. Then make sure to limit exposure to systems that handle card data by keeping all networks segmented and limiting the amount of card data stored.

– WINN OAKEY
QSA

IT CHECKLIST

PROTECTING CUSTOMER DATA

THINGS YOU WILL NEED TO HAVE:

- A documented data retention policy

THINGS YOU WILL NEED TO DO:

- Have employees acknowledge their training and understanding of the policy (3.1.a, 3.1.b, 3.1.c, 3.1.d, 3.1.e, 3.6.8, 3.7)
- Eliminate storage of sensitive authentication data after card authorization (3.2.c, 3.2.1, 3.2.2, 3.2.3)
- Mask out Primary Account Number (PAN) on customer receipts (3.3)
- Understand guidelines for handling and storing cardholder data

THINGS YOU MAY NEED TO DO:

- If Primary Account Number (PAN) data is stored for business or legal reasons, details must be masked, truncated, or secured by strong cryptography (3.4)
- PAN storage should be accessible by as few employees as possible for business or legal reasons. This includes limited access to cryptographic keys, removable media, or hardcopy of stored details (3.4.1a, 3.4.1.b, 3.4.1.c, 3.5.1, 3.6.5.a, 3.6.5.b, 3.6.5.c, 3.6.7)

REQUIREMENT 4:

SECURE DATA OVER OPEN AND PUBLIC NETWORKS

For this PCI requirement, identify where you send cardholder data. The following are common places PAN data is sent:

- Processors
- Backup servers
- Third parties that store or handle PAN
- Outsourced management of systems or infrastructure
- Corporate offices

Then you need to use encryption and have security policies in place for when you transmit cardholder data over open, public networks.

STOP USING SSL/TLS WHERE POSSIBLE

Based on vulnerabilities in web encryption, the PCI Security Standards Council has released policy stating that you need to transition from SSL and early TLS to secure versions of TLS by June 30, 2018.

SSL and TLS are widely used, so you should contact your terminal providers, gateways, service providers, vendors, and acquiring bank to determine if the applications and devices you use have this encryption protocol.
Examples of applications that likely use SSL/TLS include:

- Virtual payment terminals
- Back-office servers
- Web/application servers

If your organization has existing implementations of SSL and early TLS not necessary for regular business operations, immediately remove or discontinue all instances. Do not use any new technologies that use SSL/TLS.

THE PCI COUNCIL HAS DEEMED THAT SSL AND EARLY TLS WILL NO LONGER PROTECT CARDHOLDER DATA.

If you need to continue using SSL/TLS, consider implementing the following:

- Upgrade to a current, secure version of TLS configured not to accept fallback to SSL or early TLS
- Encrypt data with strong cryptography before sending over SSL/early TLS (i.e., use field-level or application-level encryption to encrypt data prior to transmission)
- Set up a strongly-encrypted session first (e.g., IPsec tunnel), then send data over SSL within the secure tunnel
- Check firewall configurations to see if SSL can be blocked
- Check that all application and system patches are up-to-date
- Check and monitor systems to ID suspicious activity that may indicate a security issue

Please note that organizations with existing implementations of SSL and early TLS must have a Risk Mitigation and Migration Plan in place. According to the PCI Council, this document will "detail [your] plans for migrating to a secure protocol, and also describe controls [you have] in place to reduce the risk associated with SSL/early TLS until the migration is complete."

AN AUDITOR'S PERSPECTIVE

REQUIREMENT 4:

DATA OVER OPEN AND PUBLIC NETWORKS

First off, you need to know exactly where and how you are sending cardholder data so you can know exactly what needs to be encrypted during transmission.

It's important to have a good understanding of technologies (e.g., SSL, TLS) and where your organization stands regarding your security processes. If you've already eliminated outdated processes, great. If not, have a remediation plan set and documented.

The PCI Security Standards Council has extended the SSL/TLS transition to June 30, 2018, but you really should transition away from these older technologies as quickly as possible. You might not want to lose business with customers using older browsers (e.g., SSL, TLS). in reality, there will likely be a limited negative impact on customers, if there's any at all. If I were you, I would eliminate using these outdated technologies because it's better to be safe than risk a security breach.

– WINN OAKEY
QSA

IT CHECKLIST

TRANSMITTING CARDHOLDER DATA

THINGS YOU WILL NEED TO HAVE:

- Review all locations where CHD is transmitted or received. Examine system configurations. Review all devices/systems to ensure you use appropriate encryption within your CDE. You must safeguard sensitive cardholder data during transmission over open, public networks (4.1, 4.1.a, 4.1.c, 4.1.d, 4.1.e, 4.1.f, 4.1.1)
- Use only trusted keys and/or certificates. Check inbound/outbound transmissions and verify that encryption keys and certificates are valid. Use secure configurations and proper encryption strengths. Do not support insecure versions or configurations. This means you will continually need to check latest encryption vulnerabilities and update as needed (4.1.b) (4.1.c) (4.1.d)
- Validate that POS/POI devices are not susceptible to any known exploits. Devices and software used to process credit cards need to be PCI DSS compliant (4.1.f)
- Have an in-house policy to make sure you do not send unprotected PANs via end-user messaging technologies (4.2.b)

THINGS YOU WILL NEED TO DO:

- Check all related device configuration for proper encryption. Check with vendors to make sure supplied POS/POI devices are encrypting data appropriately (4.1.f).
- Review and implement documented best practices for encryption standards (4.1.1)
- Review and implement policies and procedures for sending/receiving credit card data (4.2B)
- Examine system configuration and adjust encryption configuration as needed (4.1.a, 4.1.c, 4.1.e, 4.1.1)

THINGS YOU MAY NEED TO DO:

- Make sure TLS is enabled whenever cardholder data is transmitted or received through web based services (4.1.e)
- Check wireless network encryption standards (4.1.1)
- Examine keys and certificates (4.1.b)
- Review your Risk Mitigation and Migration Plan for environments that still need to use SSL and early TLS (4.1.g)
- Prohibit the use of WEP, an insecure wireless encryption standard (4.1.1)

REQUIREMENT 5:

PROTECT SYSTEMS WITH ANTIVIRUS

UPDATE YOUR ANTIVIRUS

Antivirus or anti-malware programs are updated on a regular basis to detect known malware. Maintaining an up-to-date anti-malware program will prevent known malware from infecting systems.

Depending on your relationship with your POS vendor, they may or may not maintain your antivirus scanning. If your vendor is not handling antivirus, it's up to you to ensure up-to-date regular scanning.

Using outside sources such as the United States Computer Emergency Readiness Team, SANS Institute, and vendor/antivirus threat feeds, merchants can identify emerging malware and attacks on systems. They can then configure systems to alert and report on suspicious activity, such as new files added to known malware directories or unauthorized access attempts.

Vigilant vulnerability management is the most effective way for you to proactively reduce the window of compromise, greatly narrowing the opportunity for hackers to successfully attack your systems and steal valuable data. As part of your vulnerability management strategy make sure to include updated antivirus software.

A VULNERABILITY IS A SYSTEM, ENVIRONMENT, SOFTWARE, OR WEBSITE WEAKNESS THAT CAN BE EXPLOITED BY ATTACKERS.

AN AUDITOR'S PERSPECTIVE

REQUIREMENT 5: ANTIVIRUS

Anti-virus software offers an additional layer of security to any system within a network. System Administrators have the responsibility of making sure their anti-virus software, including the signatures, are up to date. This applies to either a master AV server-client-based configuration or single server/workstation installations. Additionally, PCI-DSS requires AV scanning to occur on a regular basis.

PCI-DSS requires anti-virus to be installed on all systems that are commonly affected by malware (e.g., Windows). Linux servers are considered systems not commonly affected by malware. However, if a Linux server is web facing, it's highly recommended that anti-virus be installed for any web-facing Linux server. Malicious coders target Linux systems as well as Windows. The risk is too great not to run AV on web-facing Linux systems.

When System Administrators understand that anti-virus adds another line of defense for their environment, they have an advantage when it comes to securing the sensitive data it contains.

– MATT GLADE
QSA | CISSP

IT CHECKLIST

ANTIVIRUS

THINGS YOU WILL NEED TO HAVE:

- Protect all systems against malware and regularly update anti-virus software or programs
- Maintain and evaluate Audit logs with IT staff

THINGS YOU WILL NEED TO DO:

- Deploy Antivirus program on commonly affected systems
- Set Antivirus to detect and remove all known types of malicious software
- Maintain Audit logs for review
- Set Antivirus to scan automatically
- Make sure Antivirus system is updated automatically (definitions keep current)
- Make sure Antivirus cannot be disabled or altered by users (Admin access only)
- Document and review malware procedures and review with necessary staff
- Examine system configurations and periodically evaluate malware threats to system

REQUIREMENT 6:

UPDATE YOUR SYSTEMS

REGULAR SYSTEMS UPDATES AND PATCHES

Application developers will never be perfect, which is why updates to patch security holes are frequently released. Once a hacker knows he can get through a security hole, he passes that knowledge on to the hacker community who then exploits this weakness until the patch has been updated. Consistent security updates are crucial to your security posture.

Patch all critical components in the card flow pathway, including:

- Internet browsers
- Firewalls
- Application software
- Databases
- POS terminals
- Operating systems

Older Windows systems in particular can make it difficult for merchants to remain secure, especially when the manufacturer no longer supports a particular operating system or version (e.g., Windows XP). Operating system updates often contain essential security enhancements specifically intended to correct recently exposed vulnerabilities. When merchants fail to apply such updates and patches to their operating systems, the vulnerability potential increases exponentially. PCI Requirement 6.1 states merchants must “deploy critical patches within a month of release” to maintain compliance.

Be vigilant about consistently updating the software associated with your system. Don't forget about critical software installations like credit card payment applications and mobile devices. To help keep up-to-date, ask your software vendors to put you on their patch/upgrade email list.

The more systems, computers, and apps your company has, the more potential weaknesses. Vulnerability scanning is arguably the easiest way to discover software patch holes that cybercriminals would use to exploit, gain access to, and compromise an organization.

ESTABLISH SOFTWARE DEVELOPMENT PROCESSES

If you develop payment applications in-house (e.g., E-commerce websites, POS applications) you must use very strict development processes and secure coding guidelines as outlined in the PCI DSS. Don't forget to develop and test applications in accordance with industry accepted standards like the Open Web Application Security Project (OWASP).

BE VIGILANT ABOUT CONSISTENTLY UPDATING THE SOFTWARE ASSOCIATED WITH YOUR SYSTEM.

AN AUDITOR'S PERSPECTIVE

REQUIREMENT 6: SYSTEM UPDATING AND SOFTWARE DEVELOPMENT

This requirement is made up of two parts. The first part is system component and software patching, and the second part is software development.

System Administrators have the responsibility to ensure all system components (servers, firewalls, routers, workstations, etc.) and software are updated with critical security patches within 30 days of when they are released to the public. If not, these components and software are vulnerable to malware and/or security exploits.

One reason systems or software might be excluded from updates is because they simply weren't able to communicate with the update server (e.g., WSUS, Puppet), possibly resulting from a network or system configuration change that inadvertently broke the communication. It's imperative that System Administrators are alerted when security updates fail.

When developing software (e.g., web applications), it's crucial companies adopt the OWASP standard. This will guide them in their web application development process by enforcing secure coding practices and keep software code safe from malicious vulnerabilities (e.g., cross-site scripting, SQL injection, insecure communications, etc.).

Insecure communications, for example, has been in the spotlight recently since SSL and TLSv1.0 are no longer considered acceptable forms of encryption when data is being transmitted over open, public networks. The PCI Council has recently extended the migration deadline from June 30, 2016 to June 30, 2018 because so many companies require more time to migrate their systems to at least TLSv1.1 or higher. While companies work towards this goal, they are required by the PCI Council to write a Risk Mitigation/Migration Plan, detailing how they are going to mitigate this risk until they've completed the migration.

Companies need to embrace the idea of change control for their software development and system patching/updating. There are a four requirements detailed by the PCI Council of what a proper change control process must contain:

- All changes must have a documented explanation of what will be impacted by the change.
- All changes must have documented approval by authorized parties.
- Any changes to a company's production environment must undergo proper iterations of testing and QA before being released into production.
- The change control process must always include a back-out or roll-back procedure in case the updates go awry.

– MATT GLADE
QSA | CISSP

IT CHECKLIST

SOFTWARE UPDATES

THINGS YOU WILL NEED TO HAVE:

- Vendor supported programs, operating systems, and devices
- An update server (i.e., repository for systems to get updates)
- A change management process

THINGS YOU WILL NEED TO DO:

- Have a process in place to keep up-to-date with the latest identified security vulnerabilities and their threat level (6.1)
- Install all vendor-supplied security patches on all system components (6.2.a)
- Ensure all security updates are installed within one month of release (6.2.b)

THINGS YOU MAY NEED TO DO:

- Set up a manual or automatic schedule to install the latest security patches for all system components.

REQUIREMENT 7:

RESTRICT ACCESS

RESTRICT ACCESS TO CARDHOLDER DATA AND SYSTEMS

You're required to have a role-based access control system, which grants access to card data and systems to individuals and groups on a need-to-know basis. Configuring administrator and user accounts prevents exposing sensitive data to those who don't have a need-to-know.

PCI 3.2 requires a defined and up-to-date list of the roles with access to the card data environment. On this list, you should include each role, definition of each role, access to data resources, current privilege level, and what privilege level is necessary for each person to perform normal business responsibilities. Users must fit into one of the roles you outline.

HAVE A DEFINED AND UP-TO-DATE LIST OF THE ROLES WITH ACCESS TO THE CARD DATA ENVIRONMENT.

AN AUDITOR'S PERSPECTIVE

REQUIREMENT 7: RESTRICTING ACCESS

This requirement is essentially the oldest and most basic part of the PCI DSS.

Things haven't really changed for this requirement. There's no new trend or solution. But not all organizations have accurately complied with the requirement, or have even tried role-based access at all.

This is all you need to know: don't give people access who don't need it. Only give access to card systems and card data for those with a business need to know that information, and document which permissions have been granted to those persons.

– MATT HALBLIEB
QSA (P2PE) | PA-QSA (P2PE) | CISSP

IT CHECKLIST

ACCESS CONTROL

THINGS YOU WILL NEED TO HAVE:

- Written policy detailing access controls for systems in the CDE (7.1, 7.3)

REQUIRED FEATURES:

- Document access control policies based on job classification and function (7.1, 7.1.2, 7.1.3)
- Roles and privilege levels defined (7.1.1)
- "Deny all" rule in place for access control systems (7.2.3)

THINGS YOU WILL NEED TO DO:

- Detail a written policy to include access to cardholder data based on job roles with privilege level, and approval/documentation of employee access (7.1)
- Document policies in place with each employees' role/access and train employees on their specific access level (7.3)

THINGS YOU MAY NEED TO DO:

- Implement access controls on any systems where cardholder data is stored and handled (7.2.1)
- Configure access controls to only allow authorized parties and deny all others without prior approval or access (7.2.2, 7.2.3)

REQUIREMENT 8:

USE UNIQUE ID CREDENTIALS

WEAK PASSWORDS AND USERNAMES

If a username and password aren't sufficiently complex, it will be that much easier for an attacker to gain access to an environment. An attacker may try a brute-force attack against a system by entering multiple passwords (via an automated tool entering thousands of password options within a matter of seconds) until a password works.

Secure passwords should be changed every 90 days, and have at least 7 characters including an upper and lower case letter, number, and special character. Passwords that fall short of these criteria can easily be broken using a password-cracking tool.

In practice, the longer the password and more character formats, the more difficult it will be for an attacker to crack a password.

Instead of common usernames (i.e., admin, administrator, the company name, or a combination of the two), merchants should have unique usernames.

PCI requires an account lock be set to six consecutive failed login attempts within a 30 minute period. Requiring an administrator to manually unlock accounts will prevent attackers from guessing a few passwords and coming back later to try again. If an attacker only has six chances to guess the correct password, their attempts will likely fail. Once locked out, they will move on to an easier target.

SAMPLE OF COMMON BAD USERNAMES AND PASSWORDS:

USERNAME: ADMIN, USERNAME, TEST, ADMIN1, SYSADMIN, DEFAULT, GUEST, PUBLIC

PASSWORD: PASSWORD1, ADMIN1234, MONKEY!, TEST1234, CHANGEME!, LETMEIN1234

LACK OF MULTI-FACTOR AUTHENTICATION

System security should not be based solely on the complexity of a single password. No password should be considered uncrackable. That's why multi-factor authentication is the most effective solution to secure remote access, and is a requirement under PCI DSS. Unfortunately, smaller merchants often fail to implement multi-factor authentication.

Configuring multi-factor authentication requires at least two of the following three factors:

- Something only the user "knows" (e.g., a username and password)
- Something only the user "has" (e.g., a cell phone or hardware token)
- Something the user "is" (e.g., a fingerprint, ocular scan, voice print, or other biometric)

A few examples of effective multi-factor authentication for remote access include:

1. The remote user enters their username and password, and then must enter an authentication code sent to them on their cell phone.
2. The remote user enters their username and password, and then must use a unique dynamic number found on a RSA SecureID token.

Additionally, make sure that you "incorporate multi-factor authentication for all remote network access (both user and administrator, and including third-party access for support or maintenance) originating from outside the entity's network."

SOCIAL ENGINEERING IS A WAY OF MANIPULATING PEOPLE SO THAT THEY TRUST THE SOCIAL ENGINEER AND EVENTUALLY PROVIDE SOME SORT OF USABLE DATA.

AN AUDITOR'S PERSPECTIVE

REQUIREMENT 8: UNIQUE ID

This requirement is all about having unique ID information. For example, you must have your own unique ID credentials and account on your laptop, with strong password cryptography. Don't use generic accounts, shared group passwords, or generic passwords.

Today we see broader adoption of multi-factor authentication even outside the PCI realm, which is great for security. This can include your personal email, Gmail, Dropbox, and other services.

Security professionals recognize that passwords are no longer a great way to secure data. They are simply not secure enough, but are still required. You need to set strong, long passwords. A password should be at least 7 characters and complex with at least an alphabetic and numeric character.

Yet 7-character, complex passwords aren't nearly as secure as easy-to-remember long passphrases. Pick a phrase like "I eat oranges on Tuesday mornings" and add in some numbers and special characters. Your passphrase might look like this: "Ieatorangesontuesdaymorning@1235!"

In addition to strong passphrases, password manager software can help you use different passwords for all your accounts. Some password managers can even work across multiple devices and sync across the Cloud.

You really need different passwords for different services, so if one service gets compromised, it doesn't bleed into other passwords for other sites. For example, if your email account password is compromised and you use the same password across devices and websites, you have a major security problem on your hands.

– MATT HALBLIEB
QSA (P2PE) | PA-QSA (P2PE) | CISSP

IT CHECKLIST

ID CREDENTIALS

THINGS YOU WILL NEED TO HAVE:

- Multi-factor authentication for all remote access (8.3)

THINGS YOU WILL NEED TO DO:

- Monitor all remote access accounts used by vendors, business partners, IT support personnel, etc. when the account is in use (8.1.5.b)
- Disable all remote access accounts when not in use (8.1.5.a)
- Enable accounts used for remote access only when they are needed (8.1.5.a)

THINGS YOU MAY NEED TO DO:

- Implement a multi-factor authentication solution for all remote access sessions
    - Multi-factor authentication methods are as follows:
        - Something you know–password and username
        - Something you have–token
        - Something you are–fingerprint or retinal scan (8.3)

REQUIREMENT 9:

ENSURE PHYSICAL SECURITY

CONTROL PHYSICAL ACCESS TO YOUR WORKPLACE

The best way to control physical threats is through a physical security policy that includes all rules and processes involved in preserving onsite business security. If you keep confidential information, products, or equipment in the workplace, keep these items secured in a locked area. If possible, limit outsider office/business access to one monitored entrance, and (if applicable) require non-employees to wear visitor badges at all times.

Don't store sensitive information (like payment card data) in the open. For example, many hotels keep binders full of credit card numbers behind the front desk, or piled on the fax machine, for easy reservation access. Unfortunately, the collection of files is easy access to anyone within reach of the front desk or fax machine.

You also need to control employee access to sensitive areas, which must be related to an individual's job function. To comply with this requirement, you must document:

- Who has access to secured environments and their business need.
- What, when, where, and why devices are used
- A list of authorized device users
- Locations where the device is and is not allowed
- What applications can be accessed on the device

Access documentation must be kept up-to-date, especially when individuals are terminated or their job role changes.

KEEP TRACK OF POS TERMINALS

This is a huge addition to the PCI standard. Organizations that use POS systems, PIN pads, mobile devices, etc., are required to do three new things:

1. Maintain an up-to-date list of all devices (9.9.1) including physical location, serial numbers, and make/model.
2. Periodically inspect devices (9.9.2). That means ensuring device surfaces haven't been tampered with, serial numbers match, and checking that seals haven't been broken. This could be a very large task depending on the size of your organization. Whether you inspect devices every day or month is based on your tampering risk level (e.g., publically accessible 24/7 gas station terminals vs. a behind-the-counter card swipe device). Document your findings.
3. Provide staff awareness training (9.9.3) for staff who interact with card present devices on a day-to-day basis (e.g., cashiers), and record the who, what, and when for future reference. Ideally, training will help staff detect suspicious activity around a payment device. Training should include how to report suspicious behavior and what to do when third parties claim they need to work on the system. For example, rather than assuming IT came in last night to install a new device on the side of her terminal, an employee should question if it's supposed to be there and notify appropriate persons.

TRAIN YOUR EMPLOYEES OFTEN

While you may understand how to protect customer card information and your own proprietary data, your employees may not. That's why regular security trainings are so important.

Social engineering is a serious threat to both small and large businesses. A social engineer uses social interaction to gain access to private areas, steal information, or perform malicious behavior, and employees can fall for their tricks more often than you think.

For example, if a man walked into your storefront and said he was there to work on your network and needed you to lead him to the server room, would your employees think twice to further identify him and verify his presence?

Train your employees to question everything. It's better to be safe than sorry. Establish a communication and response policy in case of suspicious behavior. Train employees to stop and question anyone who does not work for the company, especially if the person tries to enter the back office or network areas.

AN AUDITOR'S PERSPECTIVE

REQUIREMENT 9: PHYSICAL SECURITY

Having electronic access on doors, using cameras to monitor all entries and exits to secure areas, implementing multiple levels of access based on a business need (See Requirement 7), and approving visitor/employee access are standard for basic security.

Today, you see more organizations hosting their systems in outsourced data centers. Data centers generally have great physical security because they pay attention to the basics. They use cameras to monitor all entires and exits, have multiple levels of access (lobby, mantrap, hallways, data floors, and cages) to segment areas and limit access to only individuals with approved access. They also use different levels of authentication requiring both a badge and biometrics (e.g. fingerprint, retina, etc.) for access.

Digital IP-based cameras are becoming more common, making it easier and more cost effective to deploy and monitor camera systems. These cameras can take snapshots of people, then send those snapshots to security supervisors for verification.

It's also necessary to protect card swipe devices. Merchants must monitor these devices for tampering or complete replacement. Make sure attackers don't substitute, bypass, or steal your terminal. You and your employees need to know what the tamper properties are (e.g., seals, appearance, weight) and test them often. Security best practice is to mount devices with tamper-resistant stands and screws.

– MARK MINER
QSA (P2PE) | PA-QSA (P2PE) | CISSP

IT CHECKLIST

PHYSICAL SECURITY

THINGS YOU WILL NEED TO HAVE:

- Policies and procedures that limit the access to your physical media and devices used for processing.

THINGS YOU WILL NEED TO DO:

- Restrict access to any public accessible network jacks in the business (9.1.2)
- Keep physical media secure and maintain strict control over any media being moved within the facility and outside of it (9.5-9.6.a)
- Keep media in a secure area with limited access (a locked office clearly marked Management Only would be one example) and require management approval before the media is moved from its secure location (9.6.1 and 9.6.3-9.7)
- Use a secure courier when sending media through the mail so the location of the media can be tracked (9.6.2)
- Destroy media in a way that it cannot be reconstructed and if the media is separated prior to destruction, keep the media in a locked container with a clear label of “To Be Shredded” or something similar (9.8.a-9.8.1.b)
- Maintain a list of all devices used for processing and train all employees to inspect devices for evidence of tampering. Training should include a process for verifying the identity of outside vendors wanting access to the machine, a process for reporting suspicious behavior around the machine, and making sure employees know not to replace devices without management approval (9.9.2.a-9.9.2.b and 9.9.3.a-9.9.3.b)

THINGS YOU MAY NEED TO HAVE:

- A set process to train employees about proper device management and a way to report any suspicious behavior around the processing device.
- A secure location to keep media, including a second secure location, if business practice is to separate media no longer needed.

REQUIREMENT 10:

IMPLEMENT LOGGING AND LOG MONITORING

IMPLEMENT LOGGING AND ALERTING

Log monitoring systems oversee network activity, inspect system events, alert of suspicious activity, and store user actions that occur inside your systems. They are your watchtower lookout and have the ability to provide the data that could alert you to a data breach. The raw log files are also known as audit records, audit trails, or event logs.

Most systems and software generate logs including operating systems, Internet browsers, POS systems, workstations, anti-malware, firewalls, and IDS. Some systems with logging capabilities do not automatically enable logging, so it's important to ensure all systems have logs turned on. Some systems generate logs but don't provide event log management solutions. Be aware of your system capabilities and potentially install third-party log monitoring and management software.

ESTABLISHING LOG MANAGEMENT

Businesses should review their logs daily to search for errors, anomalies, or suspicious activity that deviate from the norm.

From a security perspective, the purpose of a log alert is to act as a red flag when something bad is happening. Reviewing logs regularly helps identify malicious attacks on your system. Given the large of amount of log data generated by systems, it's impractical to manually review all logs each day. Log monitoring software takes care of that task by using rules to automate log review and only alert on events that might reveal problems. Often this is done using real-time reporting software that alerts you via email or text when suspicious actions are detected.

Often, log monitoring software comes with default alerting templates to optimize monitoring and alerting functions immediately. However, not everyone's network and system designs are exactly the same, and it's critical to take time to correctly configure your alerting rules at the beginning.

LOG MANAGEMENT SYSTEM RULES

Here are some event actions to consider when setting up your log management system rules:

- Password changes
- Unauthorized logins
- Login failures
- New login events
- Malware detection
- Malware attacks seen by IDS
- Scans on your firewall's open and closed ports
- Denial of service attacks
- Errors on network devices
- File name changes
- File integrity changes
- Data exported
- New processes started or running processes stopped
- Shared access events
- Disconnected events
- New service installation
- File auditing
- New user accounts
- Modified registry values

To take advantage of log management, look at your security strategy and make sure these steps are taken care of:

1. Decide how and when to generate logs.
2. Secure your stored logs so they aren't maliciously altered by cybercriminals or accidentally altered by well-intentioned employees.
3. Assign an employee you trust to review logs daily.
4. Set up a team to review suspicious alerts.
5. Spend time to create rules for alert generation (don't just rely on a template).
6. Store logs for at least one year, with three months readily available.
7. Frequently check log collection to identify necessary adjustments.

Regular log monitoring means a quicker response time to security events and better security program effectiveness. Not only will log analysis and daily monitoring demonstrate your willingness to comply with PCI DSS requirements, it will also help you defend against insider and outsider threats.

AN AUDITOR'S PERSPECTIVE

REQUIREMENT 10: AUDIT LOGS AND LOG MONITORING

It's virtually impossible to manually analyze logs beyond one or two systems. You need Security Information and Event Management (SIEM) tools to sift through logs and drill down into problems. In the past, SIEM systems were only utilized in big companies, but smaller companies now realize system monitoring can help identify attacks.

It's helpful to have a third party who specializes in log monitoring to interpret events because with each new operating system update, there is often change. If you really do have a problem, you can initiate your incident response plan (IRP).

Organizations often struggle with good log review processes. Using SIEM tools can enable you to have real-time alerting to help you recognize any current attacks. If you really do have a problem, you can initiate your incident response plan (IRP).

Also, remember that in order to correlate events over multiple systems you must synchronize system times. All systems should get their system time from one or two internal time servers which in turn receive time from a trusted external source.

– MARK MINER
QSA (P2PE) | PA-QSA (P2PE) | CISSP

IT CHECKLIST

LOGGING

THINGS YOU WILL NEED TO HAVE:

- An automated audit log tracking all security related events for all system components.
- Audit logs that track:
    - Any action taken by an individual with administrative privileges (10.2.2)
    - Failed log in attempts (10.2.4)
    - Changes to accounts – including elevation of privileges, account additions, and account deletions (10.2.5)
    - Identification of user, what the event type was, date and time of the event, whether the event was a success or failure, where the event originated from, and the name of affected data, system component, or resource (10.3.1-10.3.6)

THINGS YOU WILL NEED TO DO:

- Have a process in place to review the logs and security events at least daily, in addition to any reviews of system components as defined by the business for risk management strategy or other policies (10.6.1.b and 10.6.2.b)
- Have a process in place to respond to anomalies or exceptions (10.6.3.b)
- Keep all audit log records for at least one year and keep the last three months' logs readily available for analysis (10.7.b-10.7.c)

REQUIREMENT 11:

CONDUCT VULNERABILITY SCANS AND PENETRATION TESTING

KNOW YOUR ENVIRONMENT

A merchant's IT environment influences the kind of attacks to which they are susceptible, therefore, every security plan should be tailored to each individual network environment.

Defects in web browsers, email clients, POS software, operating systems, and server interfaces can allow attackers to gain access to an environment. Installing security updates and patches for systems in the cardholder or sensitive data environments can help correct many of the newly found defects and vulnerabilities before attackers have the opportunity to leverage them.

In the case of custom, in-house applications, code testing and independent internal penetration testing can expose many of the weaknesses commonly found in application code (especially home-grown varieties) and is the best course of defense in identifying weaknesses before deployment.

THE BASICS OF VULNERABILITY SCANNING

A vulnerability scan is an automated, high-level test that looks for and reports potential vulnerabilities. All external IPs and domains exposed in the CDE should be scanned by a PCI Approved Scanning Vendor (ASV) at least quarterly.

Typically, vulnerability scans generate an extensive list/report of vulnerabilities found and references for further research on the vulnerability. Some even offer directions for how to fix the problem.

Despite what many businesses believe, scanning is not enough. You can't just scan and sit on the report. Act quickly on any vulnerabilities discovered to ensure security holes are plugged and then re-scan to validate that the vulnerabilities have been successfully addressed.

Benefits of a vulnerability scan:

- Quick, high-level look at possible vulnerabilities
- Very affordable compared to penetration testing
- Automatic (can be automated to run weekly, monthly, quarterly)

Limitations of a vulnerability scan:

- False positives
- Businesses must manually check each vulnerability before testing again
- Does not confirm a vulnerability is possible to exploit

THE BASICS OF PENETRATION TESTING

To beat a hacker, you have to think like a hacker. Penetration testers analyze network environments, identify potential vulnerabilities, and try to exploit those vulnerabilities (or coding errors) just like a hacker would. In simple terms, analysts attempt to break into your company's network to find security holes.

A PENETRATION TEST IS AN EXHAUSTIVE, LIVE EXAMINATION DESIGNED TO EXPLOIT WEAKNESSES IN YOUR SYSTEM.

Depending on your SAQ, PCI DSS Requirement 11.3 may require an internal and external penetration test. But penetration testing isn't limited to the PCI DSS. Any company can request a penetration test whenever they wish to measure their business security.

The time it takes to conduct a penetration test varies based on network size, network complexity, and the individual penetration test staff members assigned. A small environment can be completed in a few days, but a large environment can take several weeks.

Penetration testers are well versed in:

- Black hat attack methodologies (e.g., remote access attacks, SQL injection)
- Internal and external testing (i.e., perspective of someone within the network, perspective of hacker over Internet)
- Web front-end technologies (e.g., Javascript, HTML)
- Web application programming languages (e.g., Python, PHP)
- Web APIs (e.g., restful, SOAP)
- Network technologies (e.g., firewalls, IDS)
- Networking protocols (e.g., TCP/UDP, SSL)
- Operating systems (e.g., Linux, Windows)
- Scripting languages (e.g., Python, Pearl)
- Testing tools (e.g., Nessus, Metasploit)
- Segmentation testing

Typically, penetration test reports contain a long, detailed description of attacks used, testing methodologies, and suggestions for remediation.

Benefits of a penetration test:

- Live, manual tests mean more accurate and thorough results
- Rules out false positives

Limitations of a penetration test:

- Time (1 day to 3 weeks)
- Cost (around $4,000 to $20,000)

DIFFERENCES BETWEEN VULNERABILITY SCANNING AND PENETRATION TESTING

Some mistakenly believe vulnerability scanning or antivirus scans are the same as a professional penetration test.

Here are the two biggest differences.

1. A vulnerability scan is automated, while a penetration test includes a live person actually digging into the complexities of your network.
2. A vulnerability scan only identifies vulnerabilities, while a penetration tester digs deeper to identify, then attempt to exploit vulnerabilities to get access to secure systems or stored sensitive data.

Vulnerability scans and penetration tests work together to encourage optimal network security. Vulnerability scans are great weekly, monthly, or quarterly insight into your network security, while penetration tests are a more thorough way to deeply examine network security.

ON AVERAGE, IT TOOK 1.79 SCANS AND 18 DAYS TO A FIRST SCAN AND A PASSING SCAN.

AN AUDITOR'S PERSPECTIVE

REQUIREMENT 11: PENETRATION TESTING

Whenever large infrastructure changes occur, the PCI DSS requires a formal penetration test to see if that change added any new vulnerabilities.

Even though the PCI council understand the necessity for an annual penetration test, organizations often claim no significant infrastructure changes have been made because the cost or time of a full-blown penetration test seems overwhelming.

My advice is this: first establish what your organization considers a major change. What might be a major change to a smaller organization is only a minor change in a large environment. For either size organization, if you bring in new hardware or start accepting payments in a different way, that constitutes a major change.

The next step is to establish an assessment policy. Some organizations designate a department separate from the infrastructure team to conduct self-assessments. Others hire penetration testers to conduct the assessments.

– GEORGE MATEAKI
QSA | PA-QSA | CISSP | CISA

IT CHECKLIST

VULNERABILITY SCANS AND PENETRATION TESTING

THINGS YOU WILL NEED TO HAVE:

- A process for detecting and identifying wireless access points on a quarterly basis. The method should be able to identify all of the following wireless access points:
    - WLAN cards inserted into system components
    - Mobile devices used to create wireless access points (by USB or other means)
    - Wireless devices attached to a network port or device (11.1.a-11.1.b)
- An inventory of authorized wireless access points with listed business justifications (11.1.1)
- A change-detection mechanism installed within the CDE to detect unauthorized modifications to critical system files, configuration files, or content files (11.5.a)

THINGS YOU WILL NEED TO DO:

- Run internal vulnerability scans on a quarterly basis using a qualified internal resource or qualified external third party (organizational independence must exist) and re-scan all scans until "high-risk" (as defined in the risk ranking requirement 6.1) vulnerabilities are resolved (11.2.1.a-c)
- Run quarterly external vulnerability scans (requires ASV) and re-scan until all scans obtain a passing status (no vulnerability scores over 4.0) (11.2.2.a-c)
- Run internal and external scans, using a qualified resource, after any significant change to the network, and re-scan until resolved
    - For external scans - no vulnerabilities scoring 4.0 or higher exist
    - For internal scans – all "high-risk" vulnerabilities are resolved (11.2.3.a-c)
- Configure the change-detection mechanism to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the tools to perform critical file comparisons at least weekly (11.5.b)
- Have a process in place to respond to any alerts generated by the change-detection mechanism (11.5.1)

THINGS YOU MAY NEED TO DO:

- If wireless scanning is used to identify wireless access points, the scan must be run at least quarterly (11.1.c)
- If automated monitoring is used, monitoring should generate alerts to notify personnel (11.1.d)
- Create a plan of action in the business's incident response plan for responding to the detection of unauthorized wireless access points, and take action if an unauthorized wireless access point is found (11.1.2.a-b)
- If network segmentation exists, penetration-testing procedures must confirm segmentation is operational and isolates all out-of-scope systems from systems in the cardholder data environment (11.3.4.a)

REQUIREMENT 12:

START DOCUMENTATION AND RISK ASSESSMENTS

DOCUMENT EVERYTHING

Not only do you need policies and procedures, you need to have them physically documented. Policies should be written down and easily accessible to all employees, should they have a question about security.

Documentation may also help protect your business from potential liability in the event of a breach. Having thorough and accurate documented security policies and procedures helps forensic investigators see what security measures your company has in place.

To fulfill Requirement 12.8.5 you must have a list of all third-party service providers, the PCI requirements those service providers handle, and the PCI requirements you are required to meet.

Documents you'll definitely want to have include:

- Employee manuals
- Policies and procedures
- Third-party vendor agreements
- Incident Response Plans

FOR PCI COMPLIANCE, CONSTANT AND UPDATED DOCUMENTATION OF ALL SECURITY MEASURES AND ACTIONS IS KEY.

IMPLEMENT A RISK ASSESSMENT PROCESS

PCI DSS Requirement 12.2 requires all entities annually perform a formal risk assessment that identifies critical assets, threats, and vulnerabilities. This requirement helps organizations identify, prioritize, and manage information security risks.

Merchants that take a proactive approach to security will use internal and external resources to identify critical assets, assess vulnerability threats against those assets, and implement a risk management plan to mitigate those threats.

A risk assessment should occur at least annually and after significant changes in your network and helps provide direction on what vulnerabilities you should address first. Addressing vulnerabilities decreases the time an attacker can compromise the system (i.e., window of compromise).

Remember, just because a system is vulnerable, doesn't mean it's exploitable or even likely to be exploited. Some vulnerabilities may require such a large number of preconditions that the chance of a successful attack is virtually none. Identifying the differing levels of exploitability should help an organization prioritize the actions it will take to enhance its IT security based on each identified vulnerability's perceived threat and risk level.

AN AUDITOR'S PERSPECTIVE

REQUIREMENT 12: PCI COMPLIANCE BASICS

First, make PCI compliance a regular business practice. If you view compliance as a once-a-year task, you'll probably struggle and slip in and out of compliance regularly. PCI compliance needs to be a cultural shift to common corporate culture practices. You can't bypass the process.

Second, document everything, including all processes, policies, roles, and responsibilities. Additionally, make sure all service providers sign PCI DSS compliance business agreements. Document which service providers you use, and what aspects of PCI DSS for which they are in charge. Ensure your service provider is PCI compliant on a yearly basis.

Lastly, conduct a risk assessment. Your environment may require going beyond PCI requirements to secure your payment card data. That's why you have an annual process review, documentation of the review, regular risk assessments, and updated policies. When conducting your risk assessment, look what's happening in your industry and analyze common breaches. Build your policy around what you discover.

– GEORGE MATEAKI
QSA | PA-QSA | CISSP | CISA

IT CHECKLIST

POLICY

THINGS YOU WILL NEED TO HAVE:

- Written compliance and security policies.

THINGS YOU WILL NEED TO DO:

- Each employee working in the CDE must complete annual security awareness training (12.5.3-12.6.a)

THINGS YOU MAY NEED TO DO:

- Create a company policy documenting all critical devices and services within the payment processing environment. Some examples include laptops, tablets, email/Internet usage, remote access, and wireless access technologies. This policy should include acceptable uses and storage of these technologies. The general purpose of this policy is to thoroughly explain each employee's role in the card-holder data environment. Review your lists annually (12.1-12.4)
- Create an approval process for allowing access to technologies and document which employees have current technology access. Keep lists readily available and review them annually (12.1-12.4)
- Create an incident response plan in the event cardholder data is compromised (12.10.1). The plan should include the following:
    - Roles and contact strategies in the event of compromise
    - Specific incident response procedures
    - Business continuity and recovery procedures
    - Data backup processes
    - Analysis of legal requirements in reporting possible compromise
    - Critical systems coverage and response plans
    - Notification of merchant processor and payment card brands
- Create and update a current list of third-party service providers. For example, your merchant bank, IT provider, credit card machine vendor, and credit card receipt shred-der. The following will need to be completed annually regarding your service providers:
    - Establish a process for engaging with third-party providers. Best practice would be to contact them by telephone, rather than taking inbound calls. Work by appointment with service providers onsite.
    - Obtain or update a written agreement from third-party providers acknowl-edging their responsibility for cardholder data they possess. Ensure they are PCI compliant themselves.
    - Establish a process for engaging new providers, including research prior to selecting a provider.

CONCLUSION

TOP-DOWN SECURITY

Unless someone is in charge of PCI on management's side (not just IT), PCI compliance just won't happen. Oftentimes we see companies with various groups (e.g., networking, IT, HR, Risk) expecting other departments to take charge of PCI compliance. Other times, organizations expect a QSA to be the PCI project manager, which is not feasible.

Security is not a bottom-up process. Management often tells or implies that IT should 'just get their organization secure'. However, those placed in charge of PCI compliance and security usually don't have power. Additionally, IT may not have the budget to implement adequate security (e.g., firewalls, FIM). Some may try to look for free software to fill in security gaps, but this process can be expensive due to the time it takes to implement and manage. We have experienced in some instances that the IT department wanted their PCI auditor to purposely fail their compliance evaluations so IT could receive a higher security budget. Obviously, it would have been better to focus on security from the top-down beforehand.

Management at the highest level (e.g., CEO, VP, CTO) must understand that security initiatives should come from the top and be pushed down. You can't just tell IT to 'get us compliant.' Checkbox attitudes lead to breaches. There is no check you can write to the payment card brands or an insurance company that makes you compliant. You can't just make PCI compliance go away either.

C-level management should support the process. You should be involved with budgeting, assisting, and establishing a security culture from the top level down.

OVERCOMING MANAGEMENT'S BUDGET CONCERNS

If you're having problems communicating budgetary needs to management, conduct a risk assessment before starting the PCI process. NIST 800-30 is a good risk assessment protocol to follow. At the end of this assessment, you have an idea of the probability of a compromise, how much money might be lost if compromised, and the impact a breach might have on your organization (e.g., brand damage).

Simply put, find a way to show how much a lack of security will cost the organization. For example, "if someone gains access through the system through X, this is how much it will cost us and how it will damage our brand." Consider asking marketing or accounting teams for help delivering the message in more 'bottom-line' terms. If possible, work with your QSA to come up with security controls to address the requirements to gather information on what tools you may need to implement.

CONTRIBUTORS

GARY GLOVER
MIKE SIMPSON
MATT GLADE
MATT HALBLIEB
DAVID PAGE
TREVOR HANSEN
MARK MINER
WINN OAKEY
GEORGE MATEAKI
DAVID ELLIS
ARIEL FARNSWORTH
ZACH WALKER
SAM MONSIVAIS
WHITNEY TAYLOR
BRAD NELSON

MELINDA HOWLETT
JOSH BRANDEBERRY
JEFF MCKENNA
BRANDON STEHMEIER
LINDA SILVA
DON ROBERTSON
PAUL BERRETT
AUSTIN MINER
MARJ ELDARD
JON CLARK
COLLIN MANGUM
LINDSEY HOOLEY
AMANDA HARMON
HEATHER MOON
ERIC SMITH

TERMS AND DEFINITIONS

AES (Advanced Encryption Standard): government encryption standard to secure sensitive electronic information.

ASV (Approved Scanning Vendor): a company approved by the PCI SSC to conduct vulnerability scanning tests.

CDE (Cardholder Data Environment): any individual, software, system, or process that stores, processes, transmits, or handles cardholder data.

CHD (Cardholder Data): sensitive data found on payment cards, such as an account holder name or primary account number (PAN) data.

CVV/CSC/CVC/CAV (Card Verification Value): element on a payment card that protects information on the magnetic stripe. Specific acronym depends on card brand.

DLP (Data Loss Prevention): a piece of software or strategy used to catch unencrypted data sent outside the network.

DNS (Domain Name Server): a way to translate URLs to IP addresses.

FIM (File Integrity Monitoring): a method to watch for changes in software, systems, and applications in order to detect potential malicious activity.

FTP (File Transfer Protocol): an insecure way to transfer computer files between computers using the Internet. (see SFTP)

FW (Firewall): system designed to screen incoming and outgoing network traffic.

HTTP (Hypertext Transfer Protocol): A method of communication between servers and browsers. (See: HTTPS)

HTTPS (Hypertext Transfer Protocol Over Secure Socket Layer): A secured method of communication between servers and browsers.

IDS/IPS (Intrusion Detection System/Intrusion Prevention System): a system used to monitor network traffic and report potential malicious activity.

IP (Internet Protocol): defines how computers send packets of data to each other.

IRP (Incident Response Plan): policies and procedures to effectively limit the effects of a security breach.

IT (Information Technology): anything relating to networks, computers, and programming, and the people that work with those technologies.

MFA (Multi-factor Authentication): two out of three independent methods of authentication are required to verify a computer or network user. The three possible factors are:

- Something you know (such as a username and password)
- Something you have (such as an RSA token or cell phone which gives you a new code for each login)
- Something you are (such as fingerprint or iris scan)

NAC (Network Access Control): restricts data that users, apps, and programs can access on a computer network.

NVD (National Vulnerability Database): a repository of all known vulnerabilities, maintained by NIST.

NIST (National Institute of Standards and Technology): federal agency that measures standards and maintains the NVD.

OWASP (Open Web Application Security Project): a non-profit organization focused on software security improvement, often heard in the context of "OWASP Top 10", a list of top threatening vulnerabilities.

PAN (Primary Account Number): the 14 or 16 digits that identify a payment card. Also called a bank card number.

PA DSS (Payment Application Data Security Standard): validation standard for software applications that store, process, or transmit cardholder data.

PA QSA (Payment Application Qualified Security Assessor): individual or organization qualified by the PCI SSC to conduct PA DSS audits.

PCI SSC (Payment Card Industry Security Standards Council): established in 2006 by Visa, MasterCard, American Express, Discover Financial Services, and JCB International to regulate cardholder data security.

PCI DSS (Payment Card Industry Data Security Standard): requirements put together by the PCI SSC, required of all businesses that process, store, or transmit payment card data, to prevent cardholder data theft.

P2PE (Point-To-Point Encryption): credit/debit card data encryption from the point of interaction to a merchant solution provider.

QIR (Qualified Integrator or Reseller): third party qualified by the PCI SSC to use security best practices while installing or maintaining payment systems.

QSA (Qualified Security Assessor): the individuals and firms certified by the PCI SSC to perform PCI compliance assessments.

RBAC (Role-Based Access Control): the act of restricting users' access to systems based on their role within the organization.

SAQ (Self-Assessment Questionnaire): a collection of questions used to document an entity's PCI DSS assessment results, based on their processing environment.

SFTP (Secure File Transfer Protocol): a secure way to encrypt data in transit.

SSL (Secure Socket Layer): Internet security standard for encrypting the link between a website and a browser to enable transmission of sensitive information (predecessor to TLS).

TLS (Transport Layer Security): (See SSL)

VPN (Virtual Private Network): a strategy of connecting remote computers to send and receive data securely over the Internet as if they were directly connected to the private network.

WEP (Wired Equivalent Privacy): an outdated and weak security algorithm for wireless networks.

WLAN (Wireless Local Area Network): network that links to two or more devices wirelessly.

WPA (Wi-Fi Protected Access): security protocol designed to secure wireless computer networks.

WPA2 (Wi-Fi Protected Access II): a more secure version of WPA (see WPA)

3DES (Triple Data Encryption Standard): a secure encryption standard that encrypts data three time

ABOUT SECURITYMETRICS

SecurityMetrics is a global leader in data security and compliance that enables businesses of all sizes to comply with financial, government, and healthcare mandates. Since its founding date, the company has helped over 800,000 organizations protect their network infrastructure and data communications from theft and compromise with exceptional value to customers worldwide. Among other services, SecurityMetrics offers PCI audits, penetration tests, security consulting, data discovery, and forensic analysis.

www.securitymetrics.com

securityMETRICS®