2017 SecurityMetrics Guide To

PCI DSS COMPLIANCE

A Resource For Merchants And Service Providers To Become Compliant

securityMETRICS®

FOREWORD

No matter the advances in cyber security technology and increased government cyber security initiatives and regulations, attackers continue stealing unprotected payment card data.

Some organizations have simple, easy-to-correct issues that create vulnerabilities that lead to data breaches. In other instances, organizations with intricate IT defenses and processes are overridden by an employee opening a phishing email.

We specifically designed this document as a reference guide to help merchants and service providers address the most problematic issues within the 12 PCI DSS requirements, including auditor's best practices and IT checklists. Rather than reading this guide cover to cover, we recommend using this as a resource for your PCI compliance efforts.

I hope the 2017 SecurityMetrics Guide to PCI DSS Compliance will help you better understand today's PCI requirements 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

INTRODUCTION

2017 DATA BREACH PREDICTIONS

INTRODUCTION

SecurityMetrics Payment Card Industry Forensic Investigators (PFIs) thoroughly analyze the point-of-sale (POS) or E-commerce environments of organizations that suspect a payment card data compromise.

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 the Payment Card Industry Data Security Standard (PCI DSS).

SecurityMetrics Forensic Investigators have witnessed the rise and fall of popular attack trends over 14 consecutive years. Here are three predictions for the future:

**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 throughout the course of an investigation.*

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, 2017, will likely follow similar trends from the latter half of 2016, including insecure remote access as the largest single origin of compromise. Since this intrusion technique was used in more than 39% 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) reduce the number of at-risk payment card accounts, they 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 2017, it is not likely breach trends in this arena will change.

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

Due to increased EMV implementation in 2016, the frequency of large-scale breaches seen in 2017 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. These two initiatives should contribute to a decline in the total number of compromised payment card accounts from card-present merchant environments.

However, as long as human beings are involved, no security solution is 100% secure. Employees inherently introduce the potential for inadvertent employee error, not to mention the increased popularity and sophistication of social engineering attacks. The point of vulnerability in many of 2016'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. WHILE EMV IMPLEMENTATION INCREASES, E-COMMERCE ATTACKS SHOULD INCREASE

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 require new EMV hardware. It is unreasonable to think that every merchant has implemented EMV technology. A shift towards E-commerce attacks should correlate to the percentage of EMV adoption.

While no environment will be perfectly secure in 2017, the push for EMV, updated PCI security standard requirements, and improved security technology efforts will improve the landscape of payment card industry security.

2016 SECURITYMETRICS FORENSIC TAKEAWAYS

- The average organization was vulnerable for 1,021 days
- Cardholder data was captured for an average of 163 days
- Cardholder data was exfiltrated for an average of 106 days
- 39% of organizations were breached through insecure remote access
- 22% of organizations were breached due to weak passwords
- 56% of organizations had memory-scraping malware installed on their system

TERMS TO KNOW:

VULNERABLE: A system, environment, software, and/or website can be exploited by an attacker.

CAPTURED: Data is being recorded, gathered, and/or stored from an unauthorized source.

EXFILTRATED: Unauthorized data is transferred from a system.

WINDOW OF COMPROMISE

INCREASED WINDOW OF COMPROMISE

The window of compromise starts from the date an intruder accesses a business network and ends when the breach is contained by security remediation. Based on data collected by SecurityMetrics Forensic Investigators from 2016 breaches, it took an average of 844 days from the time an organization was vulnerable for an attacker to compromise the system. The average organization was vulnerable for 1,021 days.

Nearly every organization will experience system attacks from a variety of sources. Due to inherent security weakness in systems or technology, some organizations have systems, environments, software, and/or website weaknesses that can be exploited by attackers from the day their environment is set up. In other cases, an organization becomes vulnerable because they fail to apply a security patch or make system modifications without properly updating related security protocols.

Once compromised, attackers had access to the sensitive data for an average of 163 days in 2016. This may be attributed to aggregation methods employed by data thieves. Attackers have been known to save sensitive data from malware scraping (or other tools), without using or selling the data for months to years.

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

TOP 5 CATEGORIES OF FAILED VULNERABILITIES DURING VULNERABILITY SCANS

- TLS Version 1.0 Protocol Detection
- SSL Certificate with Wrong Hostname
- Web Application Potentially Vulnerable to Clickjacking
- SSL RC4 Cipher Suites Supported (i.e., Bar Mitzvah Attack)
- SSL Self-Signed Certificate

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 that interacts with sensitive data.

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 may 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 a thorough 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 functions tested by an objective third party. This helps find vulnerabilities missed or created 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 re-scan to confirm that vulnerabilities have been addressed.

SECURITY POLICY AND EMPLOYEE TRAINING

Having clearly written policies and communicating those policies continuously to employees is 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.

THE REGULAR ROUTINE OF WORK MAKES IT EASY FOR EMPLOYEES TO FORGET CRUCIAL SECURITY INFORMATION LEARNED DURING TRAININGS.

RISK ASSESSMENT AND MANAGEMENT PLAN

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 decreases the time an attacker can compromise the system (i.e., window of compromise). Vulnerability management plans that identify your anti-virus 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 significantly more than if they had practiced proactive remediation.

IF THE BREACHED ORGANIZATION HAD BEEN COMPLIANT WITH PCI REQUIREMENTS, THE BREACH LIKELY WOULD NOT HAVE OCCURRED.

EARLY DETECTION AND CONTINUAL PROTECTION

Carefully track and manage an environment's actions to ensure early detection of a breach. System 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.

PCI DSS COMPLIANCE TRENDS

PAYMENT SECURITY

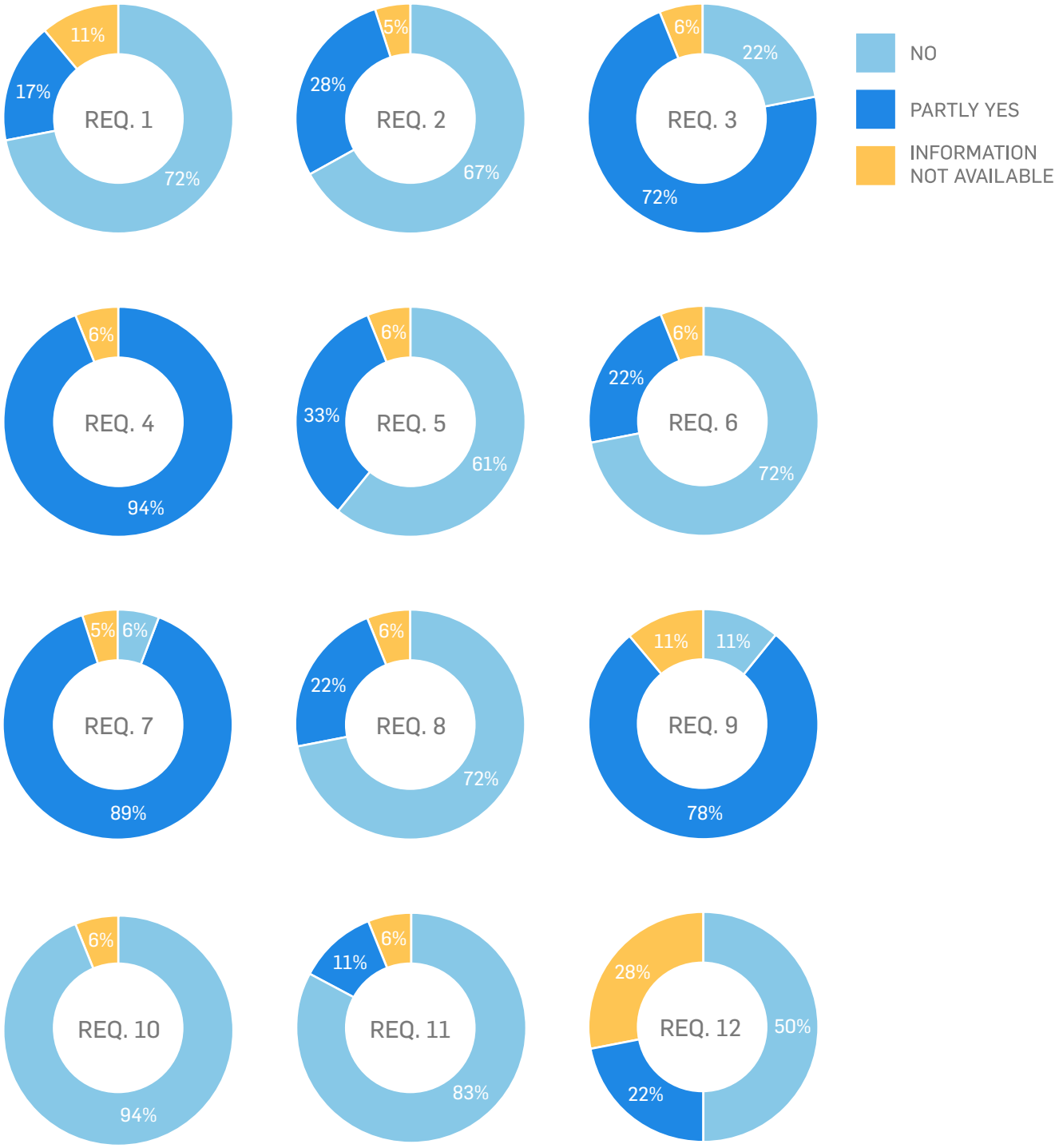
PCI DSS was established in 2006 by the major card brands (Visa, MasterCard, American Express, Discover Financial Services, and JCB International). All businesses that process, store, or transmit payment card data are required to implement the security standard to prevent cardholder data theft. The investigation 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 breached merchant at the time of data compromise was not compliant with at least 47% of the PCI DSS requirements.

NONE OF THE BREACHED MERCHANTS INVESTIGATED IN 2016 WERE FOUND TO BE FULLY PCI DSS COMPLIANT.

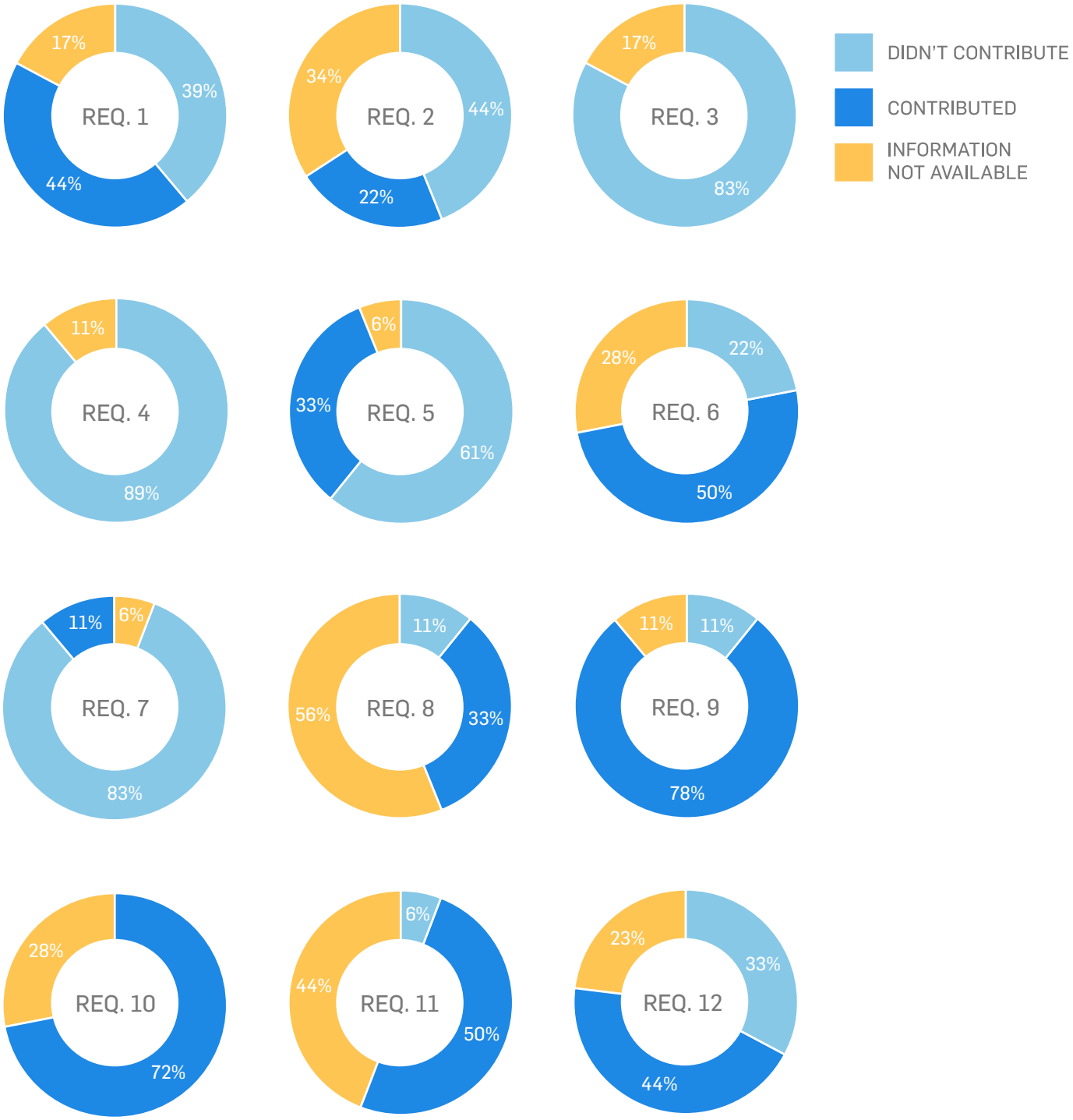
PCI DSS REQUIREMENTS IMPLEMENTED AT TIME OF COMPROMISE

These graphs discuss compliance with each requirement at the time of compromise in 2016:



NON-COMPLIANCE CONTRIBUTED TO DATA BREACH

The following is a list of how non-compliance with the different PCI requirements contributed to breaches for compromised organizations in 2016:



TOP 10 FAILING SELF-ASSESSMENT QUESTIONNAIRE (SAQ) SECTIONS

We scanned our merchant database in search of the top 10 areas where merchants struggle to become compliant. In order of least compliant requirements, these are the results:

1. **Requirement 12.5.3:** Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.
2. **Requirement 12.6:** Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures.
3. **Requirement 12.10.1:** Create the incident response plan to be implemented in the event of system breach.
4. **Requirement 12.1:** Establish, publish, maintain, and disseminate a security policy.
5. **Requirement 12.8.5:** Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.
6. **Requirement 12.8.4:** Maintain a program to monitor service providers' PCI DSS compliance status at least annually.
7. **Requirement 9.9.2.b:** Verify personnel are aware of procedures for inspecting devices and that devices are periodically inspected for evidence of tampering.
8. **Requirement 9.9.2.a:** Verify documented processes include procedures for inspecting devices and frequency of inspections.
9. **Requirement 12.4:** Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.
10. **Requirement 12.1.1:** Review the security policy at least annually and update the policy when the environment changes.

TAKEAWAYS

Unfortunately, 2016 showed some significant decreases in compliance levels when compared to previous years. None of the investigated breached merchants in 2016 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 organization been compliant with those sections of the PCI DSS, the breach likely would not have occurred.

PCI DSS 3.2: KEY CHANGES AND RECENT UPDATES

PCI DSS 3.2 (and supporting documents) was released on April 28, 2016. On October 31, 2016, PCI DSS 3.1 retired, and since then, all assessments need to use version 3.2. By February 1, 2018, organizations need to implement all new 3.2 requirements (which are currently considered best practices).

PCI DSS 3.2 received minimal changes (and future versions will likely contain similar incremental changes), which were specifically related to security threats rather than large-scale updates. Many of the 3.2 updates were minor clarifications to existing requirements or geared towards testing procedures.

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 (CDE)
- 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.

If you use SSL and early TLS and need to continue using these tools, remember not to add any new systems or technologies that use SSL and early TLS. If you need to continue them for regular business operations, the following examples illustrate some of 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.

You need to establish a formal Risk Mitigation and Migration Plan, where you detail your plans to migrate to TLS 1.2 (or better) and describe controls in place to reduce the risk associated with SSL/early TLS until the migration is complete. For example, new vulnerabilities could emerge at any time, and it's up to you to remain up to date with vulnerability trends and determine if your organization is susceptible to any known exploits.

For Point of Sale (POS) Point of Interaction (POI) terminals using SSL and/or early TLS, you need to verify that the terminals (and the SSL/early TLS termination points to which they connect) are not susceptible to any known exploits. If you find vulnerabilities in your POS POI environment, plan for migration to the latest version of TLS immediately. Although you are allowed to use SSL/early TLS for POIs after June 30, 2018, you should consider upgrading your POI environments to the latest version of TLS.

MULTI-FACTOR AUTHENTICATION REQUIRED IN OR OUT OF THE CDE (8.3)

PCI DSS 3.2 evaluates additional multi-factor authentication for administrators within a 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 (e.g., password/passphrase, PIN)
- Something you have (e.g., token device, one-time password)
- Something you are (e.g., fingerprint scan, retina scan)

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 into the CDE is from an internal network segment, you need to use multi-factor authentication. As with all the PCI DSS requirements, this is a reflection of the current threat landscape. This change helps strengthen security behind your edge firewall 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."

MULTI-FACTOR AUTHENTICATION SUPPLEMENT

In February 2017, the PCI Security Standards Council released a supplemental guide on multi-factor authentication, clarifying multi-factor authentication policies. Specifically, the MFA mechanisms should be independent of one another, so that access to one factor does not grant access to another, and the compromise of any one factor does not affect the integrity or confidentiality of any other factor.

For example, if the same set of credentials (e.g., username/password) is used as an authentication factor and also for gaining access to an e-mail account where a secondary factor (e.g., one-time password) is sent, these factors are not independent. Another faulty example is if you use a software certificate that is stored on a mobile device and protected by the same set of credentials used to log in to the device.

For good MFA implementation, you should include independence of authentication mechanisms, protection of authentication factors, and ensuring that no knowledge of the success or failure of a factor is provided to the individual until all factors have been submitted.

A common way to implement the independence of authentication factors is through a physical separation of the factors. You might also be able to use highly robust and isolated execution environments "(e.g., trusted execution environment [TEE], Secure Element [SE], and Trusted Platform Module [TPM])."

ALL NON-CONSOLE ADMINISTRATIVE ACCESS TO CDE REQUIRES MULTI-FACTOR AUTHENTICATION.

INCORPORATING DESIGNATED ENTITIES SUPPLEMENTAL VALIDATION INTO PCI DSS

PCI DSS 3.2 incorporates extra validation procedures in the Appendix. An entity is required to undergo an assessment according to this Appendix ONLY if instructed to do so by an acquirer or a payment brand. Designated entities are those who:

- Store, process, and/or transmit large volumes of cardholder data
- Provide aggregation points for cardholder data
- Have suffered significant or repeated breaches of cardholder data

If you're unsure if you're a designated entity, you likely aren't one. Acquirers and payments brands should notify you if you are and let you know what you are required to do. For example, in addition to full PCI DSS validation, designated entities must have 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 daily 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 your daily 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) outside of your organization, you are allowed to display, at a maximum, the first 6 and last 4 numbers. If you include more than this information, 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. If your business stores PAN, you're also required to encrypt and properly secure it.

REMEMBER, IF YOUR BUSINESS STORES SENSITIVE DATA, 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. Your documentation should include what qualifies as a *significant change* and these process 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., 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 should obtain a written security acknowledgment from the service provider. In this document, they need to acknowledge their responsibility to protect cardholder data that they're storing, processing, transmitting, and/or can affect your organization's security.

NEW SERVICE PROVIDER REQUIREMENTS

This section contains the most important new and revised requirements specifically for service providers. A service provider is an organization that's not a payment brand, but is directly involved in the processing, storage, or transmission of cardholder data on behalf of another organization (e.g., managed firewalls, merchant processor).

Until January 31, 2018, these new/revised service provider requirements will be considered best practice and will become requirements starting February 1, 2018.

PENETRATION TESTING REQUIREMENTS (11.3.4.1)

By February 1, 2018, service providers who use segmentation will be required to perform penetration testing on segmentation controls at least every 6 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.

This penetration testing should be performed by a qualified internal resource or third party and, if applicable, the tester should have organizational independence (though they aren't required to be a QSA or ASV). The purpose of penetration testing is to test segmentation controls/methods to verify whether they are operational and effective.

Although this requirement only applies to service providers, any organization can request a penetration test whenever they wish to measure their business security. To find security weaknesses, penetration testers analyze network environments, identify potential vulnerabilities, and try to exploit those vulnerabilities (or coding errors) just like a hacker would.

IF YOU USE SEGMENTATION AS A SERVICE PROVIDER, PERFORM PENETRATION TESTING ON SEGMENTATION CONTROLS AT LEAST EVERY 6 MONTHS AND AFTER ANY CHANGES.

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

You need to keep pace with evolving threats to your architecture by planning for and documenting updates (e.g., different algorithms/key strengths changes). Maintaining such documentation helps you detect lost or missing keys or key-management devices, and identify unauthorized additions to your cryptographic architecture.

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

Document that processes and procedures are in place to respond to security failures. Make sure staff are aware of their responsibilities in the event of a failure. If you are breached, document your organization's actions and responses to the security failure.

IF SECURITY FAILURES ARE NOT QUICKLY AND EFFECTIVELY ADDRESSED, ATTACKERS MAY USE THIS TIME TO INSERT MALWARE, TAKE SYSTEM CONTROL, AND/OR STEAL DATA FROM YOUR ENVIRONMENT.

ESTABLISH RESPONSIBILITIES FOR PCI AND DATA (12.4.1)

Executive management needs to establish responsibility for the protection of card-holder 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

Smaller organizations should add these roles to an individual's job responsibilities, while larger organizations might need to establish a PCI compliance team (e.g., a compliance team made up of IT, accounting, and management). Whichever is the case, management should give their PCI officer/team power to act and implement necessary changes to become PCI DSS compliant, as well as have monthly (or weekly) meetings with 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

SAQ UPDATES

On April 29, 2016, the PCI Security Standards Council (SSC) released the revised 3.2 version of existing SAQs, though it didn't contain new SAQ types or change SAQ descriptions. PCI DSS 3.2 brought minimal change for most SAQ types, except for SAQ A-EP, SAQ C, and SAQ D (for both merchants and service providers).

Here are the basic changes:

- SAQ A added 8 more requirements (e.g., multi-factor authentication, improved user access controls)
- SAQ A-EP added 52 more requirements (e.g., firewall configuration and documentation rules, coding procedures, intrusion detection and prevention systems, multi-factor authentication)
- SAQ B remained the same
- SAQ B-IP added 1 more requirement (e.g., multi-factor authentication)
- SAQ C-VT added 6 more requirements (e.g., multi-factor authentication, improved user access controls)
- SAQ C added 21 more requirements (e.g., multi-factor authentication, improved user access controls)
- SAQ D added 15 more requirements (e.g., multi-factor authentication, cryptographic architecture documentation, semi-annual penetration tests on segmentation)
- SAQ P2PE removed 2 requirements (e.g., masking and emailing unencrypted PAN data)

UNDERSTANDING YOUR PCI DSS RESPONSIBILITY

PCI DSS 3.2 introduced several changes, particularly about extending PCI scope and explanation of new 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. Although starting and completing your SAQ might seem daunting, 83% of SecurityMetrics customers that started their SAQ completed it.

Depending on the way you process, store, and/or handle payment data, there are different SAQs that you must choose to fill out. For example, if you do not have a storefront and all 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.

82% OF SECURITYMETRICS CUSTOMERS THAT STARTED THEIR SAQ HAVE ACHIEVED A PASSING STATUS.

PCI DSS SCOPING AND NETWORK SEGMENTATION SUPPLEMENT

In December 2016, the PCI Security Standards Council released a supplemental guide for scoping and network segmentation. The purpose of this guidance is to help organizations identify the systems that need to be considered in scope for PCI DSS, and understand how segmentation can reduce the number of in scope systems.

Organizations need to understand their environment, especially what systems are included and how those systems interact with sensitive data. You are then required to apply PCI DSS security requirements to all system components included in or connected to the CDE, which is "compromised of people, processes, and technologies that store, process, or transmit CHD or sensitive authentication data."

SCOPING YOUR ENVIRONMENT

When scoping your environment, start with the assumption that everything is in scope until it is verified that all necessary controls are in place and are actually providing effective segmentation.

When performing your annual PCI DSS scope assessment, list and confirm all connected-to systems, which are system components that:

- Directly connects to the CDE (e.g., via internal network connectivity)
- Indirectly connects to the CDE (e.g., via connection to a jump server with CDE access)
- Impacts configuration or security of the CDE (e.g., web redirection server or name resolution server)
- Provides security to the CDE (e.g., network traffic filtering, patch distribution, or authentication management)
- Segments CDE systems from out-of-scope systems and networks (e.g., firewalls configured to block traffic from untrusted networks)
- Supports PCI DSS requirements (e.g., time servers, audit log storage servers)

Without adequate network segmentation, the entire network is in scope of the PCI DSS assessment. Segmentation prevents out-of-scope systems from communicating with systems in the CDE or impact the security of the CDE. An out-of-scope system is a system component that:

- Does **NOT** store, process, or transmit CHD
- Is **NOT** in the same network segment as systems that store, process, or transmit CHD
- **CANNOT** connect to any system in the CDE
- Does **NOT** meet any criteria describing connected-to or security-impacting systems

To be considered out of scope, controls must be in place to provide reasonable assurance that the out-of-scope system cannot be used to compromise an in-scope system component. Here are some examples of controls you can use:

- Host-based firewall and/or IDS/IPS
- Physical access controls
- Logical access controls
- Multi-factor authentication
- Restricting administrative access
- Actively monitoring for suspicious network or system behavior

While not required, best practice is to implement PCI DSS controls on out-of-scope systems to prevent them from being used for malicious purposes.

TIPS FROM AN AUDITOR

PCI DSS SCOPE

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, and evaluate what people and systems are communicating with your systems. In December 2016, **the council released an information supplement regarding PCI scoping**. The document helps reinforce and clarify scoping points that have always been part of PCI scoping. The document can help you work through your annual scoping exercise, and can lead you to discovering card flows and in-scope systems that you previously ignored.

In my experience performing **PCI audits**, entities often overlook the same types of systems when doing their own PCI scoping. For instance, call centers usually pay little attention to QA systems, which often store cardholder data in the form of call recordings. Those systems are in scope for all PCI requirements!

Some simple questions can help you begin the scoping process. For example, ask yourself:

- What do you do as an organization?
- How do you collect 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? Organizations often have finance, treasury, or risk groups that have post-transaction 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. For example, 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, you don't always have full control of your 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 SecurityMetrics **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?
- How do you administer security controls on your systems?

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. In addition, if your system in the CDE initiates a communication out to a server in another zone, that server will also be in your PCI scope. There are very few exceptions to this.

TREVOR HANSEN
QSA | CISSP | CDCDP

PCI DSS 3.2 SAQ TYPES

SAQ	DESCRIPTION	NUMBER 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.

PCI DSS REQUIREMENTS

REQUIREMENT 1:

PROTECT YOUR SYSTEM WITH FIREWALLS

Network firewalls can be software or hardware technologies that provide a first line of defense to a network. Firewalls can restrict incoming and outgoing network traffic through rules and criteria configured by your organization.

HARDWARE FIREWALLS

A hardware firewall (or perimeter firewall) is typically installed at the perimeter of an organization's network to protect the internal networks from the Internet. Hardware firewalls are also used inside the environment to create isolated network segments separating the CDE from non-CDE systems.

In summary, a properly configured hardware firewall protects environments from the outside world. For example, if an attacker tries to access your network from the outside, your hardware firewall should block them.

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 FIREWALLS

It's best practice to have 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 from internal threats, particularly mobile devices that can move *outside* of the secure corporate environment.

Many devices come preinstalled with software firewalls, but for devices connecting to the cardholder data environment remotely, make sure they have a software firewall installed. For example, if a sales manager accidentally clicks on a phishing email scam, their device's software firewall should stop the malware from infecting it.

PROS	CONS
Better facilitates mobile workers outside the corporate network	Doesn't protect an entire network
Less expensive	Fewer security options
Easier to maintain	

PROPERLY CONFIGURE FIREWALLS

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 should 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 firewall(s) (i.e., 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.

In a recent data breach investigation conducted by SecurityMetrics Forensic Investigators, an organization had a sophisticated security and IT system. However, two incorrectly written firewall rules (amongst 300 pages of firewall rules, with about 100 rules on every page) essentially negated the whole firewall, leaving the entire network exposed. It was through this vulnerability that the attacker accessed their network and stole sensitive data.

IN 2016, 44% OF INVESTIGATED MERCHANTS DID NOT HAVE PROPERLY CONFIGURED FIREWALLS.

NETWORK SEGMENTATION

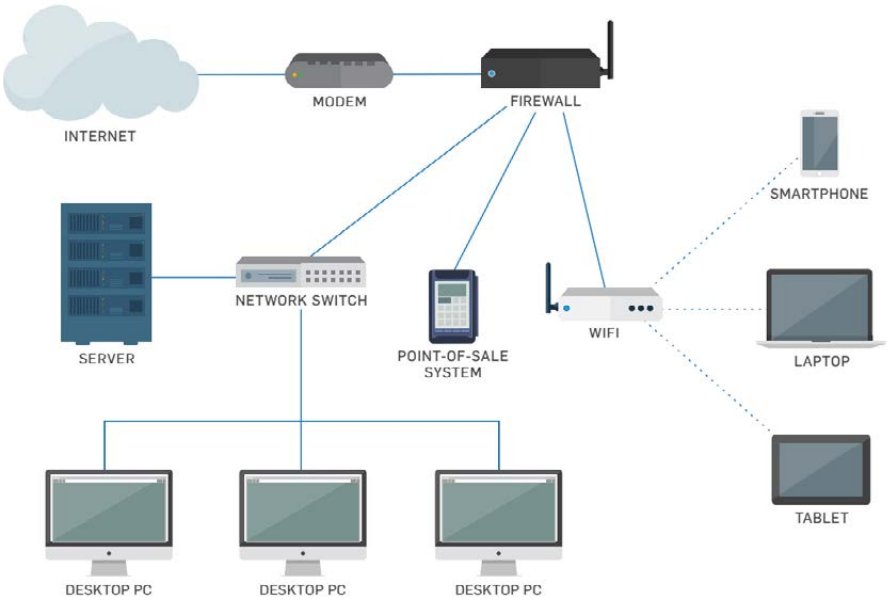
Merchants often setup large flat networks, where everything inside the network can connect to everything else. They may have one firewall at the edge of their network, but that's it. Flat networks make securing your card data extremely difficult because if an attacker gets inside of the network, they have access to everything.

Initial intrusion in many of 2016'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.

Firewalls can 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. This limits the size of the CDE and potentially lowers scope.

For example, you install and configure a multi-interface firewall at the edge of your network. From there, you create one interface on the firewall dedicated just to the systems that store/process/transmit cardholder data. If that interface doesn't allow any other traffic in or out of any other zones, this is proper network segmentation.

SAMPLE NETWORK DIAGRAM



Yes, segmentation is not necessarily required to be compliant with PCI DSS 3.2. However, if you're looking for one of the easiest ways to reduce cost, effort, and time spent on getting in-scope systems compliant, you may want to consider segmentation.

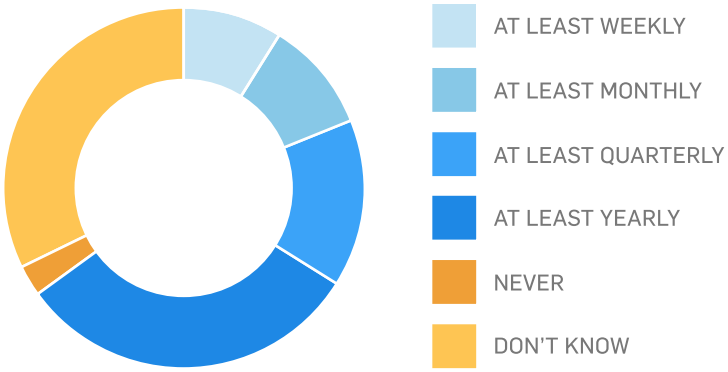
Segmentation can be extremely tricky, especially for those without a technical security background. Consider having a security professional double check all your segmentation work (e.g., segmentation checks).

TEST AND MONITOR CONFIGURATION

No matter your organizational size, rules and environments change over time. Firewall rules will need to be reviewed (and revised when necessary) over the course of a few months and at least every 6 months.

FIREWALL REVIEW STATISTICS

We asked over 350 individuals responsible for IT security and compliance decisions about how often firewall rules are reviewed by a security professional and/or third party; these are the results:



FIVE BASIC FIREWALL CONFIGURATION BEST PRACTICES

SET SECURITY: Set security settings for each switch port, particularly if using segmentation

ESTABLISH RULES: Update firewall rules if your applications and/or systems don't have proper security hardening in place (e.g., out-of-date software, default accounts and passwords)

INBOUND/OUTBOUND RULES: Decide what traffic comes in and out of your network

USE MFA: If using remote access, set up secure multi-factor authentication when granting access to sensitive networks

SEGMENT INTERNAL NETWORK: Segment different networks with switch ports (e.g., separate VLAN segments for Internet, office, CDE)

TIPS FROM AN AUDITOR

REQUIREMENT 1: ESTABLISH THOROUGH FIREWALL ARCHITECTURE

Large environments typically have firewalls in place, at least at the perimeter of the network. Make sure 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 organizations 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-validated 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. It is best to start with a *block everything* mentality, and then add exceptions as needed. PCI DSS requires you to document a valid business justification for any communication allowed to or from the CDE. Spend the time to identify specific source and destination addresses your systems need to communicate with for a given service or protocol. Don't just allow all access to the Internet, for example, because it is easier. Along the same line, if you or any third parties remotely support your environment, limit that inbound access to specific sources and protocols.

Firewalls are a first line of defense, so pay special attention to the logs and alerts firewalls generate. Often, the volume of log data can be overwhelming, so merchants turn logging off or send alert messages directly to the junk bin. It's important (and required) to review firewall logs daily to identify patterns and activity that indicate attempts to breach security. There are many good software packages available to help you deal with the volume of log data and automate alerts. This will help you pick out important data that requires you to take action.

For requirement 1, remember three things:

- Start with a *block everything* mentality, and work backwards from there
- Pay attention to what logs tell you
- Review firewall configurations frequently and adjust as necessary

DAVID PAGE
QSA | CISSP

IT CHECKLIST

FIREWALL IMPLEMENTATION AND REVIEW

THINGS YOU WILL NEED TO HAVE:

- ☐ Firewall
- ☐ Limited traffic into the CDE 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 (1.3.5)
- ☐ Documented business justification for each port or protocol allowed through the firewall (1.1.6a)

THINGS YOU WILL NEED TO DO:

- ☐ Position firewall to prohibit direct inbound and outbound traffic from the CDE (1.3)
- ☐ Create secure zone for any card data storage, must be separate from DMZ (1.3.6)
- ☐ Outbound connections from CDE must be explicitly authorized (1.3.4)
- ☐ 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 the CDE (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 continue to be a 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. Changing vendor defaults on every system with exposure to a CDE protects against unauthorized users.

Passwords must 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 vulnerabilities.

According to requirement 2.2, you must "address all known security vulnerabilities and [be] consistent with industry-accepted system hardening standards." Here are some organizations that produce good hardening guidelines:

- 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/settings have been defined and documented, it is critical 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.

TIPS FROM AN AUDITOR

REQUIREMENT 2: SYSTEM CONFIGURATION

You are required to use industry accepted configuration or hardening standards when setting up systems that are part of your PCI scope. Configuration and hardening requirements apply to all computer systems, network devices, and applications used to process or secure cardholder data. This may include things like web servers, database software, firewalls, point-of-sale systems, or workstations used to process credit card transactions.

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, changing default passwords, and configuring other security settings. Permitting anything unnecessary to remain on a system opens you up to additional risk and possible vulnerability.

Often, organizations get overwhelmed trying to understand how and where to begin implementing system configuration standards, especially in an environment that has expanded and changed over time. The first step in being able to secure your environment to meet PCI standards is to understand where credit card data is stored, processed, or transmitted. Begin by documenting the flow of CHD through your environment, making an inventory list of each system, device, or application it touches along the way. Next, look at the systems and applications that, while not directly touching the data, can affect the security of those that do. Add these devices to your list. There are several great resources available online that provide system and application hardening guidance, such as CIS, NIST, ISO, and SANS. Use this guidance to create a configuration standard that makes sense for your environment.

The key to effective system configuration and hardening is consistency. Once you have identified the different types of systems and applications that need attention, and 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 consider changes to your business or requirements, and newly discovered threats and vulnerabilities.

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

CONFIGURATION STANDARDS

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, 2.2.3, 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, 2.1.1.d, 2.1.1.e)
- ☐ 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 for web-based management and other non-console administrative access. Ensure all traffic is encrypted following current standards (2.1.1.d, 2.3)
- ☐ 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

CARDHOLDER DATA TRENDS

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 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 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, document, and follow a process of periodic data discovery cycles to recheck and ensure systems remain clean of unencrypted card information.

2016 PANSCAN® DATA ANALYSIS

Since 2010, SecurityMetrics PANscan discovered over 1.5 billion unencrypted PAN on business networks. Storage of unencrypted payment card data increases your organization's risk and liability in the event of a data breach. In 2016, we scanned over 3,400 computers and 245,000 GBs. Here are some key statistics:

- 67% of PANscan users stored unencrypted PAN data
- 5% stored track data (i.e., data inside magnetic stripe)
- Over 88 million cards found

IN THE LATEST STUDY BY SECURITYMETRICS, 67% OF PANSCAN USERS FOUND UNENCRYPTED PANS ON THEIR NETWORK.

WHERE DOES CARDHOLDER DATA HIDE

An essential part of eliminating stored card data is through using 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.

You need to create and document a current cardholder flow diagram for all card data flows in your organization. A CHD 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 CHD 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 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. For instance, it allows you to securely delete or encrypt the located unencrypted data.

	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

TIPS FROM AN AUDITOR

REQUIREMENT 3: PROTECT 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 policies to 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 it's received, timeframes to keep data, and a documented procedure to delete unnecessary payment card information that doesn't meet policy specifications.

Next, it's 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 unencrypted data is through a card data discovery tool. 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

SECURING CARDHOLDER 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, 3.6.8, 3.7)
- [ ] Eliminate storage of sensitive authentication data after card authorization (3.2.d, 3.2.1, 3.2.2, 3.2.3)
- [ ] Mask out PAN on customer receipts (3.3)
- [ ] Understand guidelines for handling and storing cardholder data

THINGS YOU MAY NEED TO DO:

- [ ] If 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 (3.4.1, 3.5, 3.5.2, 3.5.3, 3.5.4, 3.6, 3.6.1, 3.6.2, 3.6.3, 3.6.4, 3.6.5, 3.6.6, 3.6.7)

REQUIREMENT 4:

SECURE DATA OVER OPEN AND PUBLIC NETWORKS

For requirement 4, you need to 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/EARLY 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 early 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/early 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. New implementations cannot use SSL/early TLS.

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

If you need to continue using SSL/early 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."

TIPS FROM AN AUDITOR

REQUIREMENT 4:
SENDING 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/early 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, early 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, 4.1.1)
- [ ] 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)
- [ ] 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 (Appendix A2.1)
- [ ] 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 (Appendix A2)
- [ ] Review and implement documented best practices for encryption standards (4.1.1)
- [ ] Review and implement policies and procedures for sending/receiving credit card data (4.2.b)
- [ ] Examine system configuration and adjust encryption configuration as needed (4.1, 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.a, 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 (Appendix A2.2)
- [ ] Prohibit the use of WEP, an insecure wireless encryption standard (4.1.1)

REQUIREMENT 5:

PROTECT SYSTEMS WITH ANTI-VIRUS

REGULARLY UPDATE YOUR ANTI-VIRUS

Anti-virus software needs to installed on all systems commonly affected by malware. Make sure anti-virus 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 anti-virus scanning. If your vendor is not handling anti-virus, it's up to you to ensure up-to-date, regular scanning.

Using outside sources such as the United States Computer Emergency Readiness Team (US-CERT), SANS Institute, and vendor/anti-virus 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 anti-virus software.

TIPS FROM AN AUDITOR

REQUIREMENT 5:
IMPLEMENT AND UPDATE YOUR ANTI-VIRUS

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 anti-virus 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 anti-virus 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

ANTI-VIRUS UPDATES

THINGS YOU WILL NEED TO HAVE:

- [ ] Protect all systems against malware and regularly update anti-virus software or programs (5.1, 5.2.b)
- [ ] Maintain and evaluate audit logs with IT staff (5.2.c)

THINGS YOU WILL NEED TO DO:

- [ ] Deploy anti-virus program on commonly affected systems (5.1, 5.2)
- [ ] Set anti-virus to detect and remove all known types of malicious software (5.1.1)
- [ ] Maintain audit logs for review (5.2.c)
- [ ] Set anti-virus to scan automatically (5.2.b)
- [ ] Make sure anti-virus system is updated automatically (definitions keep current) (5.2.a, 5.2.b)
- [ ] Make sure anti-virus cannot be disabled or altered by users (admin access only) (5.3)
- [ ] Document and review malware procedures and review with necessary staff (5.4)
- [ ] Examine system configurations and periodically evaluate malware threats to system (5.1.2)

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.

Quickly implementing security updates is 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 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 using an unsupported operating system that doesn't receive such updates and patches, the vulnerability potential increases exponentially. 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 vulnerabilities. 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.

WEB APPLICATION FIREWALLS

In addition to updating and securing applications, web application firewalls (WAFs) should be implemented in front of public-facing web applications to monitor, detect, and prevent web-based attacks. They can also be used to perform application security assessments. Even though these solutions can't perform the many functions of an all-purpose network firewall (e.g., network segmentation), they specialize in one specific area: monitoring and blocking web-based traffic.

A WAF can protect web applications visible or accessible from the Internet, including outward facing or intranet applications involving payment card acceptance. As per PCI DSS regulations, your WAF must be up to date, generate audit logs, and either block cyber-attacks or generate a cyber security alert if an imminent attack is suspected.

PROS	CONS
Immediate response to web application security flaws	Requires more effort setting up
Protection for third-party modules used in web applications	Possibly break critical business functions (if not careful)
Deployed as reverse proxies	May require some network re-configurations

TIPS FROM AN AUDITOR

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.

Another important sub-section of requirement 6 is the need of having proper change control processes and procedures. Change control processes should include at least the following:

- Development/test environments must be separate from production with proper access control in place to enforce access rights
- Separation of duties must be implemented between personnel assigned to development/test environments and those assigned to production
- Production data (e.g., live credit card numbers, live personally identifiable information, etc.) must never be used in test/development environments
- All test data and accounts must be removed before a production environment becomes active
- Change control procedures related to implementing security patches and software modifications must be documented

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

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

When developing software (e.g., web applications), it's crucial organizations adopt industry-accepted standard or best practices for coding, such as OWASP. This will guide them in their 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, CSRF, etc.).

Insecure communications, for example, have been in the spotlight recently since SSL and TLS 1.0 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 TLS 1.2 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.

MATT GLADE
QSA | CISSP

IT CHECKLIST

SOFTWARE UPDATES

THINGS YOU WILL NEED TO HAVE:

- ☐ Vendor supported programs, operating systems, and devices (6.2)
- ☐ 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, 6.5.6)
- ☐ 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 DSS 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, the 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.

User access isn't limited to your normal office staff. It applies to anyone needing access to your systems behind the desk, such as an IT group or maintenance professionals. You need to define and document what kind of user permissions they have.

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

TIPS FROM AN AUDITOR

REQUIREMENT 7: RESTRICT ACCESS

This requirement is one of 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

ESTABLISH 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, 7.1.1, 7.1.2, 7.1.3)
- [ ] Roles and privilege levels defined (7.1, 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, 7.1.4)
- [ ] Document policies in place with each employees' role/access and train employees on their specific access level (7.1, 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 6 consecutive failed login attempts within a 30-minute period. Requiring an administrator to manually unlock accounts will prevent attackers from guessing hundreds of passwords consecutively. If an attacker only has 6 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

IMPLEMENT 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 it's 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 you know (e.g., a username and password, chip and PIN)
- Something only you have (e.g., hardware token, smartcard)
- Something only you are (e.g., a fingerprint, ocular scan)

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

- The remote user enters their username and password, and then must enter a one-time password (OTP) sent to them on their smartphone.
- The remote user enters their username and password, and then must use a unique dynamic number found on a RSA SecureID token.

Your authentication mechanisms should be independent of each other (e.g., physical separation), so that access to one factor does not grant access to another, and if one factor is compromised, it does not affect the integrity and/or confidentiality of any other factor.

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."

IF A REMOTE ACCESS APPLICATION CONFIGURATION ONLY REQUIRES THE USER TO ENTER A USERNAME AND PASSWORD, THE APPLICATION HAS BEEN CONFIGURED INSECURELY.

TIPS FROM AN AUDITOR

REQUIREMENT 8: USE UNIQUE ID CREDENTIALS

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. As a system administrator it is also a best practice to have a r*egular* account that is used for day-to-day work on your laptop and a different administrative account when performing administrative functions on the systems you manage.

After January 31, 2018, all non-console administrative access to in-scope systems will require multi-factor authentication. Organizations need to start planning and testing now to make sure they are ready for this deadline.

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. To meet PCI requirements, a password must be at least 7 characters and complex with both alphabetic and numeric characters.

Yet 7-character, complex passwords aren't nearly as secure as easy-to-remember long passphrases. Pick a phrase like "I like eating oranges" and add in some numbers and special characters. Your passphrase might look like this: "iLeO35!"

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–one-time password
  - [ ] Something you are–fingerprint or retinal scan (8.3)

REQUIREMENT 9:

ENSURE PHYSICAL SECURITY

CONTROL PHYSICAL ACCESS TO YOUR WORKPLACE

Employees may think physical security only applies after hours. However, most data thefts (e.g., social engineering attacks) occur in the middle of the day, when staff is too busy with various assignments to notice someone walking out of the office with a server, company laptop, phone, etc.

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.

THE MAJORITY OF PHYSICAL DATA THEFTS TAKE ONLY MINUTES IN PLANNING AND EXECUTION.

Keep an up-to-date inventory of all removable devices including a list of authorized users, locations the device is assigned or is not allowed, and what applications are allowed to be accessed on the device. Best practice is to not allow these devices to leave the office, but if they do, consider attaching external GPS tracking technology and remote wipe on all laptops, tablets, external hard drives, flash drives, and mobile devices.

In addition, make sure all workstations have an automated timeout/logout on computers and devices (e.g., a password-protected screensaver pops up on a computer after a set amount of time). This helps discourage thieves from trying to access data from these workstations when employees aren't there.

KEEP TRACK OF POS TERMINALS

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 you should ensure device surfaces haven't been tampered with, make sure serial numbers match, and check 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 every 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 the terminal, an employee should question if it's supposed to be there and notify appropriate persons.

TRAIN YOUR EMPLOYEES EARLY AND 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 fall for their tricks more often than you think.

For example, if someone walked into your storefront and said they were there to work on your network and needed you to lead them to the server room, would your employees think twice to further identify them and verify their 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.

PHYSICAL SECURITY BEST PRACTICES

Most physical security risks can be prevented with little effort. Here are some suggestions to improve your physical security:

- While working on your risk analysis, look for physical security risks
- Lock all office doors and applicable equipment (e.g., mobile devices) when not in use day and night
- Require passwords to access computers and mobile devices
- Encrypt your data or don't store data on these devices
- Use screensavers and privacy monitors on computers
- Install and use blinds in all office windows
- Keep logs of who goes in and out
- Keep track of devices that go in and out
- Have policies in place for stolen equipment (establish a good incident response plan)
- Train staff against social engineering
- Limit access to CHD through role-based access
- Have staff report suspicious people and devices
- Monitor sensitive areas with video cameras and store the video logs for appropriate durations

TIPS FROM AN AUDITOR

REQUIREMENT 9: IMPROVE 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 entries and exits, have multiple levels of access (e.g., 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) 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 and 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

IMPROVING 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, 9.5.1, 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, 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, 9.8.1)
- [ ] 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, 9.9.3)

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

SYSTEM LOGS AND ALERTING

System event logs are recorded tidbits of information regarding the actions taken on computer systems like firewalls, office computers, printers, etc.

Log monitoring systems (e.g., Security Information and Event Management [SIEM] tools) 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 can 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.

LOGS ARE ONLY USEFUL IF THEY ARE REGULARLY REVIEWED.

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 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:

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

ORGANIZATIONS SHOULD REVIEW THEIR LOGS DAILY TO SEARCH FOR ERRORS, ANOMALIES, OR SUSPICIOUS ACTIVITY THAT DEVIATES FROM THE NORM.

TIPS FROM AN AUDITOR

REQUIREMENT 10: AUDIT LOGS AND LOG MONITORING

Given the large amount of log data generated by systems, it's virtually impossible to manually analyze logs beyond one or two systems. You likely need 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.

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

Also, remember that 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.

PCI DSS version 3.2 requires service providers to implement a process to detect and respond to failures of critical security controls in a timely manner. You need to be able to detect these failures and have defined incident responses in place. These response plans need to not only address the response to fix the problem but also identify risks that were created by the failure, identify root causes, document the lessons learned, and implement any changes necessary to prevent the failures from happening again.

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

IT CHECKLIST

LOGGING AND LOG MANAGEMENT

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, 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 TESTS

UNDERSTAND 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 are required to be scanned by a PCI Approved Scanning Vendor (ASV) at least quarterly.

PCI DSS requires two independent methods of PCI scanning: internal and external scanning. An external vulnerability scan is performed outside of your network, and it identifies known weaknesses in network structures. An internal vulnerability scan is performed within your network, and it looks at other hosts on the same network to identify internal vulnerabilities.

Typically, these 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.

PROS	CONS
Quick, high-level look at possible vulnerabilities	False positives
Very affordable compared to penetration testing	Businesses must manually check each vulnerability before testing again
Automatic (can be automated to run weekly, monthly, quarterly)	Does not confirm a vulnerability is possible to exploit

THE BASICS OF PENETRATION TESTING

Just like a hacker, penetration testers analyze network environments, identify potential vulnerabilities, and try to exploit those vulnerabilities (or coding errors). 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.

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

In addition to annual penetration tests, you'll want to perform a formal penetration test whenever large infrastructure changes occur to see if that change added any new vulnerabilities.

PERFORM A PENETRATION TEST AT LEAST YEARLY AND AFTER MAJOR NETWORK CHANGES.

PROS	CONS
Live, manual tests mean more accurate and thorough results	Time (1 day to 3 weeks)
Rules out false positives	Cost (around $4,000 to $20,000)
Automatic (can be automated to run weekly, monthly, quarterly)	Does not confirm a vulnerability is possible to exploit

DIFFERENT TYPES OF PENETRATION TESTING

NETWORK PENETRATION TEST

The objective of a network penetration test is to identify security issues with the design, implementation, and maintenance of servers, workstations, and network services.

Commonly-identified security issues include:

- Misconfigured software, firewalls, and operating systems
- Outdated software and operating systems
- Insecure protocols

SEGMENTATION CHECK

The objective of a segmentation check is to identify whether there is access into a secure network because of a misconfigured firewall. Basically, segmentation checks confirm if segmentation was set up properly.

Commonly-identified security issues include:

- TCP access is allowed where it should not be
- ICMP (ping) access is allowed where it should not be

APPLICATION PENETRATION TEST

The objective of an application penetration test is to identify security issues resulting from insecure development practices in the design, coding, and publishing of the software.

Commonly-identified security issues include:

- Injection vulnerabilities (SQL injection, cross-site scripting, remote code execution, etc.)
- Broken authentication (The log-in panel can be bypassed)
- Broken authorization (Low-level accounts can access high-level functionality)
- Improper error handling

WIRELESS PENETRATION TEST

The objective of a wireless penetration test is to identify misconfigurations of authorized wireless infrastructure and the presence of unauthorized access points.

Commonly-identified security issues include:

- Insecure wireless encryption standards
- Weak encryption passphrase
- Unsupported wireless technology
- Rogue/open access points

SOCIAL ENGINEERING

The objective of a social engineering assessment is to identify employees that do not properly authenticate individuals, follow processes, or validate potentially dangerous technologies. Any of these methods could allow an attacker to take advantage of the employee and trick them into doing something they shouldn't.

Commonly-identified issues include:

- Employee(s) clicked on malicious emails
- Employee(s) allowed unauthorized individuals onto the premises
- Employee(s) connected a randomly discarded USB to their workstation

VULNERABILITY SCANNING VS. PENETRATION TESTING

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

Here are the two biggest differences:

- A vulnerability scan is automated, while a penetration test includes a live person actually digging into the complexities of your network.
- A vulnerability scan only identifies vulnerabilities, while a penetration tester digs deeper to identify the root cause of the vulnerability that allows 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 SECURITYMETRICS CUSTOMERS 1.68 SCANS AND 11 DAYS TO ACHIEVE A PASSING SCAN.

TIPS FROM AN AUDITOR

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 understands 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 SCANNING 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, 11.1.c)
- [ ] 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 quarterly internal vulnerability scans using a qualified internal resource or external third party (organizational independence must exist) and re-scan all scans until *high-risk* (as defined in req. 6.1) vulnerabilities are resolved (11.2.1)
- [ ] 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)
- [ ] 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)
- [ ] 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)
- [ ] If network segmentation exists, penetration-testing procedures must confirm segmentation is operational and isolates all out-of-scope systems from systems in the CDE (11.3.4.a)

REQUIREMENT 12:

START DOCUMENTATION AND RISK ASSESSMENTS

REGULARLY DOCUMENT BUSINESS PRACTICES

Not only do you need policies and procedures, you also need to have them 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 include in your security policy:

- 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.

ESTABLISH A RISK ASSESSMENT PROCESS

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.

Organizations 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 so many 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.

THE PURPOSE OF THE RISK ANALYSIS IS TO HELP ORGANIZATIONS DOCUMENT POTENTIAL SECURITY VULNERABILITIES, THREATS, AND RISKS.

PCI DSS TRAINING BEST PRACTICES

If you think your employees know how to secure cardholder data and what they're required to do, you're sadly mistaken. In fact, most breaches originate from employees. Although most workers aren't malicious, they often either forget security best practices or don't know exactly what they're required to do.

Unfortunately, many hackers will take advantage of human error to gain access to sensitive data. For example, thieves can only steal laptops if workforce members leave them in plain sight and unattended. Hackers can only access networks because workforce members set up easy-to-guess passwords. And the list goes on.

To help protect sensitive data, employees need to be given specific rules and regular training to know how to protect PAN data. Regular training (e.g., brief monthly training) will remind them of the importance of security, especially keeping them up to date with current security policies and practices. Here are some tips to help employees protect your sensitive data:

- **Set monthly training meetings:** focus each month on a different aspect of a data security, such as passwords, social engineering, email phishing, etc.
- **Give frequent reminders:** these could be sent out in an email, newsletter, during standup meetings, and/or PCI DSS security webinar that includes tips for employees
- **Train employees on new policies ASAP:** newly hired employees should be trained on security and PCI policies as quickly as possible
- Make training materials **easily available:** Intranet sites are a great way to provide access to training and policy information
- **Create incentives:** reward your employees for being proactive
- **Regularly test employees:** create an environment where employees aren't afraid to report suspicious behavior

TIPS FROM AN AUDITOR

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.

Finally, conduct a risk assessment. Your environment may require going beyond PCI requirements to secure your payment card data. That's why you need 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

CORPORATE POLICY AND DOCUMENTATION

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 (12.6, 12.6.1)

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 CDE. 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 IT provider, credit card machine vendor, and credit card receipt shredder. The following will need to be completed annually regarding your service providers (12.8, 12.8.1):
  - [ ] 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 (12.8.3)
  - [ ] Obtain or update a written agreement from third-party providers acknowledging their responsibility for cardholder data they possess. Ensure they are PCI compliant themselves (12.8.2)
  - [ ] Establish a process for engaging new providers, including research prior to selecting a provider

PCI DSS BEST PRACTICES

HOW TO MANAGE A DATA BREACH

You can't afford to be unprepared for a data breach's aftermath. It's up to you to control the situation and protect your brand in the wake of a data breach's potentially devastating hold on reputation. The following steps will help you successfully stop information from being stolen, mitigate further damage, and restore operations as quickly as possible.

START YOUR INCIDENT RESPONSE PLAN

A business typically learns they've been breached in one of four ways:

- The breach is discovered internally (via review of intrusion detection system logs, event logs, alerting systems, system anomalies, or anti-virus scan malware alerts).
- Your bank informs you that you've been breached based on reports of customer credit card fraud.
- Law enforcement officials discover the breach while investigating the sale of stolen credit card accounts on the black market.
- A customer complains to you because your organization was the last place they used their card before it began racking up fraudulent charges.

If you suspect a data breach, here are your objectives: stop information from being stolen and repair your systems so a breach won't happen again. This begins by executing your incident response plan.

A well-executed incident response plan can minimize breach impact, reduce fines, decrease negative press, and help you get back to business more quickly. In an ideal world and if you're following PCI DSS requirements, you should already have an incident response plan prepared and employees trained to quickly deal with a data breach situation.

But if there is no plan, employees scramble to figure out what they're supposed to do, and that's when big mistakes are made. For example, if employees wipe a system without first creating images of the compromised systems to learn what occurred and to avoid re-infection.

PRESERVE EVIDENCE

When an organization becomes aware of a possible breach, it's understandable to want to fix it immediately. However, without taking the proper steps and involving the right people, you could inadvertently destroy valuable forensic data used by investigators to determine how and when the breach occurred, and what to recommend to properly secure the network against the current attack or similar future attacks.

When you discover a breach, remember:

- Don't panic
- Don't let your failure to not panic lead you to hasty actions
- Don't wipe and re-install your systems (yet)
- Do follow your incident response plan

SET YOUR INCIDENT RESPONSE PLAN INTO MOTION IMMEDIATELY AFTER LEARNING OF A SUSPECTED DATA BREACH.

CONTAIN THE BREACH

Your first priority at this point in time is to isolate the affected system(s) to prevent further damage until your forensic investigator can walk you through the more complex and long-term containment.

1. **Disconnect** from the Internet by pulling the network cable from the firewall/router to stop the bleeding of data.
2. **Document** the entire incident. This documentation should include the following information:
    - How you learned of the suspected breach
    - The date and time you were notified
    - How you were notified
    - What you were told in the notification
    - All actions you take between now and the end of the incident
    - Date and time you disconnected systems in the card data environment from the Internet
    - If and when you disabled remote access
    - If and when you changed credentials/passwords
    - All other system hardening or remediation steps taken
3. **Disable** (do not delete) remote access capability and wireless access points. Change all account passwords and disable (not delete) non-critical accounts. Document old passwords for later analysis.

4. **Change** access control credentials (usernames and passwords) and implement highly complex passwords: 7+ characters that include upper and lower case, numbers, and special characters. (Avoid passwords that can be found in any dictionary, even if you are substituting special characters in place of letter characters.)
5. **Segregate** all hardware devices in the payment process from other business critical devices. Relocate these devices to a separate network subnet and keep them powered on to preserve volatile data.
6. **Quarantine** instead of deleting (removing) identified malware found by your anti-virus scanner for later analysis and evidence.
7. **Preserve** firewall settings, firewall logs, system logs, and security logs (take screenshots if necessary).
8. **Restrict** Internet traffic to only business critical servers and ports outside of the payment-processing environment. If you must reconnect to the Internet before an investigator arrives, remove your credit card processing environment from any devices that must have Internet connectivity and process credit cards via dial-up, stand-alone terminals obtained from your merchant bank until you consult with your forensic investigator.
9. **Contact** your merchant processing bank (if you haven't already) and let them know what happened.
10. **Consider** hiring a law firm experienced in managing data breaches. It won't be cheap, but they may help you avoid pitfalls that could damage your brand. Your law firm may hire a forensic firm to immediately investigate and ensure you've properly contained the breach. If the credit card brands have issued a mandate that a forensic investigation must occur, you will be required to hire a PCI forensic investigator to perform the investigation, even if you or your law firm has already employed a non-PFI forensic firm.

START INCIDENT RESPONSE MANAGEMENT

ASSEMBLE YOUR INCIDENT RESPONSE TEAM

A data breach is a crisis that must be managed through teamwork. Assemble your incident response team immediately. (Hopefully you've already met and discussed roles during crisis practices and initiated your incident response plan.)

Your team should include a team leader, lead investigator, communications leader, C-suite representative, office administrator, human resources, IT, attorney, public relations, and breach response experts. Each brings a unique perspective to the table with a specific responsibility to manage the crisis.

CONSIDER PUBLIC COMMUNICATIONS

Proper communication is critical to successfully managing a data breach, and a key function of the incident response team is to determine how and when notifications will be made.

Several states have legislated mandatory time frames that dictate when a merchant must make notifications to potentially affected cardholders. You should be aware of the laws in your state and have instructions in your incident response plan that outline how you will make mandated notifications.

Identify in advance the person within your organization (perhaps your inside legal counsel, newly hired breach management firm, C-level executive, etc.) that is responsible for ensuring the notifications are made timely and fulfill your state's specific requirements. Your public response to the data breach will be judged heavily, so think this through.

STALLING MAY NOT BE IN YOUR BEST INTEREST

Your customers will discover if you keep important breach information from them. If the media marks your brand untrustworthy for withholding information, that label could end up hurting you worse than the other effects of the data breach. Some companies fall into the, "Let's make sure we know exactly what's going on before we say anything at all" trap, but excessive delays in releasing a statement may be seen as an attempted cover-up.

Providing some information to your customers is usually better than saying nothing at all. You can always provide updated statements as needed on your website. In all cases regarding public statements, seek the guidance of your legal counsel.

MAKE SURE EMPLOYEES DON'T ANNOUNCE THE BREACH BEFORE YOU DO

Poorly informed employees can often circulate rumors. As a team, establish your media policy that governs who is allowed to speak to the media. Designate a spokesperson and ensure employees understand they are not authorized to speak about the breach.

Depending on your circumstances, you may find it beneficial to withhold from the rank and file employees the fact that your company has suffered data breach until shortly before any public statements are made.

DISCLOSURES OF THE BREACH WITHIN THE COMPANY AND TO THE PUBLIC NEED TO FOLLOW THE ADVICE FROM YOUR LEGAL COUNSEL.

Your incident response team should craft specific statements that target the various audiences, including a holding statement, press release, customer statement, and internal/employee statement. These should be communicated to appropriate parties that could potentially be affected by the breach, such as third party contractors, stockholders, law enforcement, and ultimately cardholders.

Your statements should address questions like:

- Which locations are affected by the breach?
- How was it discovered?
- Is any other personal data at risk?
- How will it affect customers and the community?
- What services or assistance (if any) will you provide your customers?
- When will you be back up and running, and what will you do to prevent this from happening again?

Explain that you are committed to solving the issue and protecting your customer's information and interests. Where you deem appropriate, you could offer an official apology and perhaps other forms of assistance such as one year of free credit monitoring.

INVESTIGATE, FIX YOUR SYSTEMS, AND IMPLEMENT YOUR BREACH PROTECTION SERVICES

Management of a data breach doesn't end with your public statement. Now comes the hardest part: investigating and fixing everything. Luckily, you're not alone. Your PFI will perform the majority of the investigation and then provide recommendations on how to repair your environment to ensure this doesn't happen again.

BRING AFFECTED SYSTEMS BACK ONLINE

After the cause of the breach has been identified and eradicated, you need to ensure all systems have been hardened, patched, replaced, and tested before you consider re-introducing the previously compromised systems back into your production environment. During this process, ask yourself these questions:

- Have you properly implemented all the recommended changes?
- Have all systems been patched, hardened, and tested?
- What tools/reparations will ensure you're secure from a similar attack?
- How will you prevent this from happening again? (Who will respond to security notifications and be responsible to monitor security, IDS/IPS, and firewall logs?)

SET YOUR BREACH PROTECTION SERVICES INTO MOTION

It's now time to enact your breach protection services, if you have one. This is a data breach reimbursement program that helps cover some of the costs of a data breach. Breach protection can alleviate an enormous amount of stress surrounding data breaches, as you'll know you won't have to bear the entire brunt of expenses related to the breach.

BE PREPARED FOR THESE COSTS

Obviously, the financial examples presented below will change based on: your size, how many customer cards were stolen, how hackers got into your organization, if you were willfully aware of your vulnerabilities, whether you have breach protection services etc.

If breached, you may only be liable for a few of these fines, or you could be expected to pay even more than listed below. It depends on a number of factors. Along with possible legal fines, federal/municipal fines, increased monthly card processing fees, you may have to pay for the following:

DATA BREACH FINES	
Merchant processor compromise fine:	$5,000 – $50,000
Card brand compromise fees:	$5,000 – $500,000
Forensic investigation:	$12,000 – $100,000
Onsite QSA assessments following the breach:	$20,000 – $100,000
Free credit monitoring for affected individuals:	$10 – $30/card
Card re-issuance penalties:	$3 – $10 per card
Security updates:	$15,000+
Lawyer fees:	$5,000+
Breach notification costs:	$1,000+
Technology repairs:	$2,000+
TOTAL POSSIBLE COST:	**$50,000 – $773,000+**

MAKE SURE IT DOESN'T HAPPEN AGAIN

A key part of a successful breach response is what you learned from the breach. After the dust has settled, assemble your incident response team again to review the events in preparation for the next attack. Incorporate the lessons you've learned and ask, "How can we improve the process next time?" And then revise your incident response plan. Don't forget to communicate your commitment to data security to the media, even after you've repaired the damage.

INSTALL AND MONITOR FILE INTEGRITY MONITORING SOFTWARE

If you haven't already, install file integrity monitoring software on all critical systems because it will alert you when changes to important files have been made.

For example, you can see that yesterday at 3 AM a file was added to an obscure folder when no one was updating your system. Chances are, it's malware that was added when you visited an infected website, and it wasn't detected by anti-malware. After doing a little searching following discovery, it's much easier to remove that piece of malware off your system.

You should regularly review (e.g., at least daily) and monitor logs generated by your FIM software. Set up logs to alert system administrators in an event of suspicious activity. If a system detects suspicious activity, such as when a new software program is installed in an odd location, or if someone attempts to log in 300 times in a row, log alerting can tip off the internal IT team to begin an investigation.

INSTALL INTRUSION DETECTION SYSTEMS

One of the reasons data breaches are so prevalent is a lack of proactive, comprehensive security systems dedicated to monitoring system irregularities, such as IDS, host intrusion detection systems (HIDS), network intrusion detection systems (NIDS), etc.

Using this software can help identify a suspected attack and help you locate security holes in your network that gave the attackers access in the first place. Without the knowledge derived from IDS logs, it can be very difficult to find system vulnerabilities or determine if cardholder data was accessed/stolen.

By setting up alerts on an IDS, you can be warned as soon as suspicious activity occurs and be able to significantly mitigate compromise risk within your organization, and you may even stop a breach in its tracks.

From a legal standpoint, an organization could also use the information stored by their IDS in a breach court case to show they did as much as possible to contain the breach.

Additionally, forensic investigators (like SecurityMetrics forensic investigators) use information gleaned from client IDS tools to investigate breaches. IDS tools reveal data such as how the hacker got in, how long they remained in the system, and when they exported data. This helps investigators determine exactly how much sensitive data was exported, and what the organization must do to secure system vulnerabilities.

Keep in mind that an IDS isn't preventive. Similar to a private investigator, an IDS doesn't interfere with what it observes. It simply follows the action, takes pictures, records conversations, and alerts the client. For more preventative measures, you might consider an Intrusion Prevention System (IPS), which is an extension of IDS and is usually paired together. However, unlike IDS, it will prevent and block many intrusions that are detected.

AN IDS COULD HELP YOU DETECT A SECURITY BREACH AS IT'S HAPPENING IN REAL TIME.

PCI DSS BUDGET

To become PCI compliant, you'll need to spend money. The cost of PCI compliance entirely depends on your organization. Here are a few variables that will factor in to the cost of your overall compliance:

- **Your business type** (e.g., franchise, service provider, or mom and pop shop): Each business type will have varying amounts of transactions, cardholder data, environment structure, risk levels, merchant levels, and/or service provider levels, which means different requirements.
- **Your organization size:** Typically, the larger the organization, the more potential vulnerabilities it has. More staff members, more programs, more processes, more computers, more cardholder data, and more departments means more cost.
- **Your organization's environment:** The type of processing systems, the brand of computers, the kind of firewalls, the model of back-end servers, etc. can all affect PCI cost.
- **Your organization's dedicated PCI staff:** Even with a dedicated team, organizations usually require outside assistance or consulting to help them meet PCI requirements.

The following are estimated PCI budgets:

SMALL ENTITY	
Self-Assessment Questionnaire (SAQ)	$50-$200
Vulnerability Scanning	$100-$150 per IP address
Training and policy development	$70 per employee
TOTAL POSSIBLE COST	**$220+**

MEDIUM/LARGE ENTITY	
Onsite audit	$40,000+
Vulnerability scan	$800+
Penetration testing	$5,000+
Training and policy development	$5,000+
TOTAL POSSIBLE COST	**$50,800+**

Keep in mind this budget doesn't include remediation security measures, such as firewalls, encryption, updating systems and equipment, etc. However, this is far cheaper than paying for a data breach.

TIPS FROM AN AUDITOR

PCI DSS RESPONSIBILITIES AND CHALLENGES VARY FOR EACH ORGANIZATION

The PCI Data Security Standard does not change based on the size of the company or the company's cardholder data environment to which it is being applied, but the challenges faced when applying PCI DSS to environments of differing sizes do seem to vary based on size.

It has been my experience that small merchants or service providers tend to struggle documenting and following policies and procedures. During a PCI DSS assessment, the QSA will first look to see that required policies and procedures are in place and will then verify by review of documentation and system configurations that policies and procedures are being followed. Smaller merchants or service providers whose CDE consists of only a few machines and who have a small relatively stable staff involved in maintaining the CDE often do not see the benefit of or feel they do not have the time to document procedures. Unfortunately, it is not uncommon to perform a renewal assessment for a merchant or service provider that had been compliant in the past, but due to unexpected employee turnover and lack of documentation, have neglected to perform tasks required to maintain compliance throughout the year.

Small merchants should, at the minimum, set up a PCI email user or active directory account 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, semiannual 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.

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 prior to implementing changes to the CDE. Unfortunately, due to their size and the different entities involved in the management of the CDE, 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 or one stakeholder will make decisions that have unintended consequences for other stakeholders in the CDE.

To help address some of these concerns, the new PCI DSS requirement (Requirement 12.4.1) requires service providers to define a charter for the organization's PCI DSS compliance program that requires executive management involvement. While this is only required for service providers, it is recommended that larger merchants follow this requirement as well.

Large organizations and service providers should establish an official PCI charter that describes the management and accountability of the organizations compliance program (Requirement 12.4.1). Additionally, they should implement internal audit procedures to ensure security practices are properly in place throughout the year (Requirement 10.8 and 12.11). PCI compliance cannot be just an annual audit event.

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 log centralization and daily review. 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 checkmarks on their SAQ.

MIKE SIMPSON
QSA

CONCLUSION

CONCLUSION

CREATE A SECURITY CULTURE

Unless someone oversees PCI on management's side (not just IT), PCI compliance just won't happen. We often 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. If you are a C-level executive, you should be involved with budgeting, assisting, and establishing a security culture from the top level down.

OVERCOME 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 to 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
PARKER NELSON
BRAD NELSON
MELINDA HOWLETT
JOSH BRANDEBERRY
JEFF MCKENNA
BRANDON STEHMEIER
DON ROBERTSON
PAUL BERRETT
TYLER FARR
FORREST BUTLER
SIDNEY CLARK
RICH BUSHNELL
JON CLARK
COLLIN MANGUM
ANDREW GARRETT
LINDSEY HOOLEY
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 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 one-time password token)
- Something you are (such as fingerprint or iris scans)

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.

WAF (Web Application Firewall): an application firewall that monitors, filters, and/or blocks HTTP traffic to and from a web application.

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

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

WPA (Wi-Fi Protected Access): a 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.

consulting@securitymetrics.com

801.705.5656

securityMETRICS®