Security First, PCI Compliance Second

Creating a security program that exceeds any compliance standard

By Jeffrey Man, Security Strategist, Tenable Network Security
February 17, 2015

Revision 2

Table of Contents

I. Introduction 3

II. A brief history of the Payment Card Industry Data Security Standard 3
The goal of the PCI DSS 3
Who must adhere to the PCI DSS? 3
Two types of entities 3
Compliance 5

III. Six major goals 6
PCI requires technology solutions 7
Goal #1: Build and maintain a secure network 7
Goal #2: Protect cardholder data 8
Goal #3: Maintain a vulnerability management program 8
Goal #4: Implement strong access control measures 9
Goal #5: Regularly monitor and test networks 9
Goal #6: Maintain an information security policy 9

IV. What's new in PCI DSS v3.0 10
Types of changes 10
New requirements 10
New "business as usual" theme 11

V. PCI myths, realities, and truths 12
Myths 12
Realities 13
Security Truths 14

VI. How to make PCI work for you 15
Recommendations 15

VII. How Tenable can help with security 16
Tenable product portfolio 16
Nessus®: Meet PCI requirements 17
Nessus Cloud: Meet ASV scan requirements 17
PVS™: Enforce your cardholder data environment 18
SecurityCenter CV™: Maintain ongoing compliance 18
Mapping Tenable solutions 18

VIII. Other Resources 20

IX. Terminology 21

X. Endnotes 22

XI. Bibliography 22

I. Introduction

This document briefly describes the Payment Card Industry Data Security Standard (PCI DSS), the standard technical and operational requirements to protect cardholder data, and Tenable's recommendations for compliance with the standard.

If you are already familiar with PCI DSS, you'll want to read section IV which explains what is new in version 3.0.

If you are looking for guidance for complying with PCI, read sections *V: PCI myths, realities, and truths*, *VI: How to make PCI work for you*, and *VII: How Tenable can help with security*.

PCI DSS compliance can be complicated, but when you practice security continuously every day, compliance comes naturally. If you follow this "security first, compliance second" approach, you probably are already secure and compliant with PCI DSS. By living, breathing, and practicing security, compliance becomes second nature.

II. A brief history of the Payment Card Industry Data Security Standard

The Payment Card Industry Data Security Standard (PCI DSS) is the standard for the security and protection of cardholder data globally. In the early 2000s, Visa, the leading brand in the industry, led the way in defining a Cardholder Information Security Program, which became a de facto standard for other card brands. By 2004, the major card brands agreed on a common set of security standards that were based on the Visa program. And in 2006, they created the Payment Card Industry Security Standard Council (PCI SSC), an independent governing board comprised of five major card brands: Visa, MasterCard, American Express, Discover Financial Services, and JCB International. The Council issues and updates the PCI DSS and publishes other standards associated with the payment card/payment acceptance industry.

The goal of the PCI DSS

The PCI DSS provides guidelines for the protection and security of cardholder data and payment transactions data. The objectives of the standard are described in the DSS introduction:

> *The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect cardholder data. PCI DSS applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD).*[1]

PCI DSS provides a complete set of security standards for merchants and providers as a common baseline and criteria. The standard includes both technical and operational requirements, and applies to any entity that impacts the security of cardholder data. The standard was created with guidance from the software industry and manufacturers of devices used in PCI transactions.

Who must adhere to the PCI DSS?

The major credit card brands require PCI DSS compliance by all businesses that are involved in the transmission, processing, or storage of payment card data, including merchants and third-party service providers that may impact the security of the data. These businesses must demonstrate that compliance on an annual basis.

Two types of entities

Many types of companies are subject to compliance with PCI DSS, and are grouped into two broad categories:

Merchants - Any entity that accepts payment cards from any of the five PCI SSC members as payment for goods and/or services. Merchants include traditional brick and mortar establishments, e-commerce vendors, and other services such as mobile payment systems, taxi cabs, hotels, flea market vendors, and corporate e-stores. In short, any organization that accepts credit cards is subject to PCI. The number of vendors is staggering; the number of merchants using Visa is up to 6 million and growing every day. Compliance is monitored by the merchant's acquiring bank.

Service Provider – A business entity that is not a payment brand but that is directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity. These companies are typically in between merchants and banks and may not even realize that they are involved in security of the cardholder data environment (CDE). For example, this includes companies providing "redirect" payment services, such as PayPal Pro and CyberSource. Compliance is monitored by the card brands.

Many banks must be PCI DSS compliant. Any bank that runs ATMs and issues debit cards must be compliant, and banks that issue credit cards must be compliant; these are called **issuing banks**. Banks that do business with the merchants must be compliant; these are called **acquiring banks**. Merchants must report PCI DSS compliance to their acquiring banks, and service providers must report their compliance to the actual card brand. And while all these banks are subject to PCI DSS, no one is currently validating them — they do not have to answer to a higher entity for an annual compliance validation. This is a loophole that needs to be plugged because this lack of accountability could translate into a bank not following the PCI DSS completely.

The PCI DSS categorizes each type of complying organization by "level" (commonly referred to as "large" or "small") which is based on the volume of credit card transactions processed for a specific card brand on an annual basis. For example, Visa specifies four levels:

U.S. PCI DSS Compliance Status

VISA

Merchant Level	Estimated Population Size	Estimated % of Visa Transactions	PCI DSS Compliance Validation	Validated Not Storing Prohibited Data
Level 1 Merchant (>6M)	450	50%	97%	100%
Level 2 Merchant (1-6M)	972	13%	88%	100%
Level 3 Merchant (e-commerce only 20,000 – 1M)	4,095	< 5%	61%	N/A
Level 4 Merchant (<1M)	~ 5,000,000	32%	Moderate**	TBD

*** As of June 30, 2014**
****Level 4 compliance is moderate among stand-alone terminal merchants, but lower among merchants using integrated payment applications**

Compliance

Any business that is subject to PCI DSS must validate their compliance on an annual basis. The Council provides both a *Report on Compliance Reporting Template* and *Self-Assessment Questionnaires* (SAQ) for annual compliance reporting.

The first step in assessment is to determine the **scope** of the CDE by identifying locations, systems, and data flows that impact cardholder data. Scoping must be fully documented to demonstrate how it was determined and to enumerate all systems within the scope of the PCI DSS assessment.

The Council recommends (but doesn't require) **network segmentation** to reduce the scope of an assessment. Segmentation is a method used to isolate the CDE from the rest of a business' network systems so that an assessment is conducted only on those systems (physical, virtual, wireless, and cloud-based) that store, process, or transmit cardholder data. A complete understanding of business processes, and documentation such as data flow diagrams and system charts can help determine the boundaries of segmentation.

A validation audit against the specific PCI DSS requirements can have a significant impact on a merchant. If a company doesn't fully embrace the impact that successful PCI security standard implementation can have on their overall security posture – not simply for the protection of credit card data, but for the protection of their entire enterprise – they're missing the point that PCI DSS compliance is not about annual compliance paperwork, but about daily habits. PCI DSS is about best security practices in general; it's not just about what the PCI Council says is important – the principles of compliance can be applied equally effectively to cybersecurity policies for all IT operations.

Compliance validation

Large companies – both merchants and service providers – must validate compliance by having an independent assessment performed either by a Qualified Security Assessor (QSA) or a properly trained internal resource certified by the PCI Council as an Internal Security Assessor (ISA). The assessor uses the *Report on Compliance Reporting Template* to document and validate the compliance assessment.

Self-assessment

Every other company (small merchants) that is subject to PCI DSS compliance is required to self-assess using the appropriate *Self-Assessment Questionnaire*. For the majority of companies that must do self-assessment questionnaires, they are left on their own to interpret the requirements and to complete the questionnaire with guidance only from the PCI DSS standards. Consequently, an attitude may develop that thinks of PCI compliance as just another audit; after completing one audit, that information is fine for the next audit. This attitude reflects a desire to reduce the burden of PCI DSS compliance. But that's missing the point; the overarching principle is that you have to secure your environment and your data, not just fulfill PCI compliance with minimal effort.

The small or Level 4 merchants (earning less than a million dollars) are the least likely to have IT staff or a substantial investment in security solutions. This category of merchant is usually ignored, or they are reliant on a third party solution provider to set them up with PCI DSS certified POS systems — where the merchant has minimal contact with payment cards, and hopes that the provider is taking care of transactional security. This can be problematic when the solution provider isn't following the PCI DSS and/or the small merchant is a franchise operation that is carrying the banner of a large, well-known, publicly recognized merchant. If the small merchant is under the belief that they don't have to do PCI DSS, a lack of adherence to the PCI DSS can easily enable a breach of card data.

Validating a third party

If all a merchant does is e-commerce and the payment processing is completely redirected to third party processors, compliance validation is mostly reduced to validating that the payment processor is PCI DSS compliant. The "service provider" must demonstrate its compliance to the card brands. From a security perspective, this shifts the responsibility for the security of card data to a trusted third party who is in the payment processing business and takes the necessary actions to secure the data on behalf of its clients.

Compliance is protection

For every company that makes it into the news for a security breach, there are probably 20 - 50 other smaller businesses that are also affected by attacks. The payment industry continues to experience breaches with the goal of stealing payment card information for fraudulent purposes. Scrimping on PCI DSS compliance only contributes to this trend.

A lot of merchants ask, “Why is PCI DSS so complicated; why is it so hard to follow?” These organizations struggle to meet all of the requirements and successfully demonstrate compliance. On the other hand, other merchants recognize that “PCI DSS is a just a starting point.” They know that PCI DSS represents a bare minimum approach and that a “real” security-focused program would go much further and require much more. How can the standard define the minimum requirements yet be so difficult to achieve? Primarily because security is about an attitude/posture/mindset rather than the achievement of a perceived state. Security is something you do continuously, not something to merely check off on a to-do list. PCI DSS is not just an annual task, it is a security lifestyle.

III. Six major goals

The PCI DSS is not hard to understand. The standards are broken into just 6 straight forward goals. The 6 goals are further subdivided into 12 major requirements. And those 12 major requirements enumerate sub-requirements that drill down into the details of implementation.

The six major goals of PCI DSS outline a security framework that works for any environment and company, not just the PCI industry. They describe a solid data protection program for anyone in the information security business. The goals and requirements are summarized in the following table.

Goals	PCI DSS Requirements
Build and maintain a secure network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect cardholder data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability management program	5. Use and regularly update antivirus software or programs 6. Develop and maintain secure systems and applications
Implement strong access control measures	7. Restrict access to cardholder data by business need to know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly monitor and test networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an information security policy	12. Maintain a policy that addresses information security for all personnel

PCI DSS covers the whole enterprise, including systems, people, processes, and different types of technologies that make up your network. And of course, there is a cost associated with security; PCI implies that for each of the 12 requirements you have different technology or security solutions in place. These solutions are not *required* to meet the 12 requirements, but in many cases the requirements ask you to evaluate how well you are implementing these types of technology solutions.

PCI requires technology solutions

Each of the 12 major requirements identifies one or several different technologies that are expected to be in place or mandatory to meet the spirit of that requirement. These technologies are summarized in the following table.

PCI DSS Requirements	Required Technologies/Solutions
Requirement 1: Install and maintain a firewall configuration to protect cardholder data	Firewalls, routers, switches, virtualization
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	Servers, workstations, virtualization appliances, VPN, POI, POS, Payment applications
Requirement 3: Protect stored cardholder data	File/disk drive encryption, encrypted databases
Requirement 4: Encrypt transmission of cardholder data across open, public networks	VPN, SSL certs, OpenSSL, Data Loss Protection
Requirement 5: Protect all systems against malware and regularly update antivirus software or programs	Antivirus, Anti-malware, Whitelisting
Requirement 6: Develop and maintain secure systems and applications	Web app testing tools, Web application firewalls
Requirement 7: Restrict access to cardholder data by business need to know	Access control systems
Requirement 8: Identify and authenticate access to system components	Secure remote access, SSH, VPN, 2FA, authentication mechanism
Requirement 9: Restrict physical access to cardholder data	Key pad/PIN entry, CCTV, badge readers, off-site storage
Requirement 10: Track and monitor all access to network resources and cardholder data	Centralized logging solutions, log parsers, SIEM, NTP
Requirement 11: Regularly test security systems and processes	Wireless detection, pen testers, vulnerability scanners, ASV, FIM, IDS/IPS
Requirement 12: Maintain a policy that addresses the information security for all personnel	Risk assessment process, incident response training, security awareness training, CISO, Security Operations

The intent of each goal and its requirements are discussed in the following six sections.

Goal #1: Build and maintain a secure network

PCI DSS compliance starts with a secure network — building secure servers, workstations, and systems attached to the network. All systems should go through hardening or configuration processes — systems cannot just be plugged in out of the box. By knowing your data flows, you can securely control the flow of information through and out of your network. Everything should be managed securely and on a daily basis to maintain the same level of security that you ensure at the outset.

In the past, theft of financial records required a criminal to physically enter an organization's business site. Now, many payment card transactions (such as debit in the U.S. and "chip and pin" in Europe) use PIN entry devices and

computers connected by networks. By using network security controls, entities can prevent criminals from virtually accessing payment system networks and stealing cardholder data.

This goal includes two requirements as guidance:

1. Install and maintain a firewall configuration to protect cardholder data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.

Goal #2: Protect cardholder data

Once you have a secure network, the next goal is to know your data – what data qualifies as cardholder data – secure it. This principle of data protection could apply to any sensitive data, whether it's company, proprietary, secret or customer data.

Data must be protected anywhere it is *stored, transmitted* or *processed*, as outlined in this goal's two requirements:

3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data across open, public networks.

Requirement 3 deals with the security of cardholder data at rest) while Requirement 4 deals with the security of cardholder data during transmission (in flight, in motion) over open, public (e.g. untrusted) networks. If you have implemented segmentation in your network to create a cardholder data environment (CDE), then the rest of your network would fall into the category of open, public or untrusted. In that case, you must protect the data in transit over your internal network.

Technically, encryption is only one option to meet the PCI requirement for obfuscating data both at rest and in flight. Encryption is not a silver bullet; just because you can't read it doesn't mean it cannot be stolen. A hacker can steal the key to the encryption to unlock its contents. And even when you use encryption, the data is still exposed to intruders when it is being encrypted or decrypted. Other means of protection include VPN, SSL certificates, data loss protection, and OpenSSL.

Goal #3: Maintain a vulnerability management program

Vulnerability management is the process of systematically and continuously finding weaknesses in an organization's payment card infrastructure system. This includes security procedures, system design, implementation, or internal controls that could be exploited to violate system security policy.

You must have a vulnerability management program, and you must keep systems and applications secured. This is where Tenable has a long history and can help an organization meet its security goals. A cyclical pattern recurs in the IT industry: systems and applications are put out there and then people figure out how to break them - they find bugs and poorly configured systems that they can exploit. So businesses must have a complimentary cycle of discovering problems and patching/fixing them. It's a never ending cycle that must be ongoing and robust. Remediation includes:

- Keeping systems and applications updated and patched, regularly and consistently
- Replacing an operating system when it goes out of support
- Knowing what vulnerabilities can impact your systems by monitoring independent sources of vulnerability information and fixing the problems
- Writing secure programs when developing internal applications, especially web applications

Two requirements for a vulnerability management program cover a lot of ground:

5. Use and regularly update antivirus software or programs
6. Develop and maintain secure systems and applications

Goal #4: Implement strong access control measures

Access control provides ways for a business to permit or deny access to sensitive cardholder data. Access must be granted on a business need to know basis. Physical access control entails the use of locks or restricted access to paper-based cardholder records or system hardware. Logical access control – user versus administrator privileges, encrypted access or two-factor authentication for remote access - permits or denies use of PIN entry devices, a wireless network, PCs and other devices. It also controls access to digital files containing cardholder data.

Access control has been a major issue for several recent breaches, in terms of controlling the users as well as their access levels. Many levels of control can be implemented, such as restricting administrative privileges, only using administrative privileges when necessary, applying the "need to know" principle for access, establishing strong user account controls and procedures. The requirements of this goal stipulate:

7. Restrict access to cardholder data by a business need to know.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data.

Goal #5: Regularly monitor and test networks

This PCI DSS section talks about watching, being diligent, and monitoring everything that's going on in the network with the intent of detecting unusual activity and anomalies that are not normal.

And how do you know what is normal? The only way to define normal is to regularly monitor *all* activity so that you can identify activity that is the exception. And even if an unusual activity turns out to be legitimate, from a network perspective, you still need to monitor continuously so that you can investigate unusual events.

Security controls for today's networks include:

- Vulnerability scanning, both inside and outside
- Continuous monitoring of everything
- Capturing all activity logs
- Reviewing all the data on an ongoing basis to detect malicious activities and recover from them
- Penetration testing to assess the effectiveness of your security program and to make sure you haven't missed anything
- Saving all the data as forensic evidence
- Remediation of findings as soon as possible

Physical and wireless networks are the glue connecting all endpoints and servers in the payment infrastructure. Vulnerabilities in network devices and systems present opportunities for criminals to gain unauthorized access to payment card applications and cardholder data. Monitoring and testing are critical to tracking dishonest activity:

10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes

Goal #6: Maintain an information security policy

A strong security policy sets the tone for security affecting an organization's entire company, and it informs employees of their expected duties related to security. Writing down policy is something that most people hate to do, but it's a necessity for complying with PCI DSS. A written security policy provides standards that everyone in the organization must meet and procedures that must be followed consistently to meet those standards. PCI DSS primarily mandates written *procedures*; if you have a certain practice, a way of rolling out a new system, a hardening methodology or a billing process, you have to document it — not only so you can do things consistently, but so you can reproduce a process. Anyone who replaces you or who is hired as your business grows must be able to repeat processes consistently and in a secured manner.

The requirement states:

12. Maintain a policy that addresses information security for all personnel

Maintenance is critical – these are living, breathing documents that must be kept up to date on a regular basis. Update your security policy every time there is a change, so you are not scrambling once a year to remember changes and to update the written document under a deadline.

IV. What's new in PCI DSS v3.0

Types of changes

In 2014, the Council issued version 3.0 of the PCI standards. This version includes significant changes which fall into three basic categories:

- **Clarification** – To ensure understanding of a requirement's intent

  The majority of changes fall into this category. The Council actually went through and changed the order of many requirements so that the standards flow more logically.

- **Additional Guidance** – To further explain, define, and/or instruct with information on given topics

  The Council provided a lot of detail to explain why specific requirements exist or to clarify what they are looking for with certain requirements.

- **Evolving Requirement** – To keep the standard up-to-date with emerging threats

  These changes update requirements, provide more explanation, and provide technology details.

The majority of changes in version 3.0 are intended to help the validation process, and to provide clear, informative context to the spirit and rationale for each requirement. There isn't much that is really "new" for companies that have taken the "security first" approach to PCI and have not attempted to do just the bare minimum. Much of the clarification answers the common question, "Where does it say I have to do that?"

It will be challenging to provide complete inventories (along with corresponding network and business process/data flow diagrams of the payment card environment) where this hasn't been accomplished before. Small merchants and service providers will also find it difficult to navigate and choose from the 9 different Self-Assessment Questionnaires, whether they are going it alone or relying upon a solution vendor for guidance.

For readers already familiar with PCI DSS, the following two sections summarize the changes in version 3.0.

New requirements

There are five new requirements in Version 3.0.

New Requirements in PCI DSS Version 3.0	
6.5.10	Address broken authentication and session management coding vulnerabilities
8.5.1	Service providers with remote access to customer premises must use unique credentials for each customer
9.9	Physically inspect Point of Introduction (POI) devices to detect tampering or substitution
11.3	Implement a methodology for penetration testing
12.9	Service providers acknowledge in writing that they are responsible for the cardholder data that they transmit, process, store, or could impact security of the data or CDE

In terms of what's new, there is now a grace period for adoption of five specific requirements. The standard itself will be fully in place by January 1, 2015, but companies must comply with these 5 requirements by June 30, 2015. By creating a grace period, the Council has acknowledged that working with the revised requirements is a challenge and that most organizations will need additional time to implement them.

It's interesting that requirement 8.5.1 addresses service providers or third parties who have remote access to customer premises and that requires them to use unique credentials for each customer. This was actually one of the problems in a recent breach — credentials were stolen by a third-party and the thieves essentially used the same user credentials to log in to all the merchants that they supported. If 8.5.1 has been in place earlier, perhaps that breach would not have happened.

Requirement 9.9 addresses the physical inspection of point of introduction (POI) devices. This is an important requirement because one of the technologies that is being promoted within PCI to make things more secure is the idea of encrypting the data when it's swiped at a POI device. Of course, after implementing encryption technology, the next logical step is for intruders to steal the device or to break into it to get the encryption. A key is included within the encryption, and that key is what gives hackers the ability to steal the information. The Council acknowledges that this is preemptive, to put physical inspection in place as a future control when these devices are encrypted.

New "business as usual" theme

Probably the most significant news in the PCI standard is recognition that the 12 major requirements roll up to about 400 specific controls that must be followed on a *real time continuous basis*.

The entire standard suggests that you're doing all of these things on an ongoing basis. But to avoid confusion, the Council published an entire section on *Best Practices for Implementing PCI DSS into Business-as-Usual Processes*[2] to reiterate that complying with these requirements should be "business as usual." Security should be something that is part of your daily routine. And they categorize the specifics into two recommendations:

- Monitor everything, especially the security technology that is protecting everything within your network
- Respond to events that occur or issues you discover and deal with them accordingly

As an evolutionary or iterative process, when things happen, you have to go back and evaluate how the system affected the security of your payment card data. You can extrapolate that back to any type of security program, not just PCI. You need a methodology to determine how the PCI DSS changes, the newly discovered vulnerabilities, and new attacks impact your operations. You need processes for change management, for updates, and for remediation. And again, this must be done on an ongoing basis. It must be done with everything in line and in a formal way. Anything that is done in security should be repeatable, and that requires formality and documentation.

The Council explains what "business as usual" is:

1. Monitoring security controls to ensure that they are operating effectively and as intended

2. Ensuring that all failures in security controls are detected and responded to in a timely manner

3. Reviewing changes to the environment prior to completion of the change, and:

    - Determining the potential impact to PCI DSS scope (for example, a new firewall rule that permits connectivity between a system in the CDE and another system could bring additional systems or networks into scope for PCI DSS)
    - Identifying PCI DSS requirements applicable to systems and networks affected by the changes (for example, if a new system is in scope for PCI DSS, it must be configured per system configuration standards, including FIM, AV, patches, audit logging, etc., and must be added to the quarterly vulnerability scan schedule)
    - Updating PCI DSS scope and implement security controls as appropriate

4. Formally reviewing the impact to PCI DSS scope based on organizational changes

5. Periodically holding reviews and issuing communications to confirm that PCI DSS requirements are in place and personnel are following secure processes

6. Reviewing hardware and software technologies at least annually to confirm that they continue to be supported by the vendor and can meet the organization's security requirements, including PCI DSS

The business as usual guidelines are not PCI DSS requirements, but they are excellent recommendations for practicing "security first and compliance second."

V. PCI myths, realities, and truths

To understand PCI DSS, it helps to understand some common attitudes and misconceptions about the standards. Qualified Security Assessors often hear merchants expressing the following beliefs about PCI which are not necessarily true. Check your understanding of the standards against these myths, confirm the realities of PCI, and adjust any unfounded attitudes with our list of security truths.

Myths

If you are PCI compliant you won't get hacked

A lot of vendors feel that if they are PCI compliant, they have no problems and they won't be hacked. But that's not always the case. PCI takes a lot of effort — even more so in version 3 — of paying attention to the third-party services and making sure that they are PCI compliant too.

Segmentation and scope reduction are the key

Much of the PCI DSS process, especially the marketing from vendors, revolves around "scope reduction" and "reducing the burden" of PCI DSS compliance, rather than focusing on the security benefits of practices such as segmentation (or security-in-depth) which can make it harder or more time-consuming for hackers to navigate through your network to critical systems and payment card data. Not taking the right approach/attitude when implementing segmentation has been a key factor in many recently reported breaches. If the focus had been on securing the data rather than "easing the burden," many of these breached retailers would not be in the news.

Memory scraping malware is the latest "new" attack

Backoff is a type of malware that targets point of sale systems. A point of sale system essentially is a cash register, the computer that's operating as a cash register at retail locations, running what's called a payment application. The processing of the payment – from the swiping of your credit card to the transmission of that information back to the bank for approval – is all controlled by a payment application that is running on the computer. That is a point of sale system.

The Backoff malware attacks those specific types of systems by "memory scraping," or taking all the information that's in the computer's memory and saving it out to a file. In many recent and successful breaches, hackers installed Backoff in multiple point of sale systems, lifted data out to similar systems, and provided all that data to the bad guys.

One of the PCI myths is that recent breaches are all accomplished with Backoff malware, and that we are seeing attacks based on new technology. But that's not entirely true. What's being exploited is old technology; Backoff is actually targeting the Windows XP operating system which went out of support early in 2014.

In theory, no company should be running Windows XP. But there are a lot of systems in the payment card industry which were built with an embedded operating system – Windows XP. An embedded operating system is a stripped down version of the operating system, a barebones version that only includes the essentials for running an application. And it's another myth that because it's embedded, Windows XP is not as vulnerable to attack – because there is not as much interaction with the system and updating is not required.

In actuality, embedded Windows XP is still in support through 2016. And it's this operating system that's really targeted by Backoff malware. So old technology and old vulnerabilities are being exploited. What's new is that hackers have figured out a way to get this malware into point of sale systems and have been very successful at reaping the rewards.

Realities

Many of those myths are based on misconceptions about PCI DSS. Consider the following realities that impact PCI compliance, usage, and methodologies.

Scoping is a major task

If compliance sounds like a complex problem to a business, you can understand why there would be so much emphasis on limiting the scope for PCI DSS compliance. Scoping your cardholder data environment is often a major undertaking and requires deep knowledge of all business and IT processes and data flows. The PCI DSS actually requires companies to have a documented process for determining what is and what is not part of the CDE (or simply "in scope"). They must also be able to present evidence and results of the methodology used to determine the scope of PCI in their enterprise.

Segmentation is not required

Closely related to scope is segmentation, and there are two issues with segmentation. First, PCI DSS does not require segmentation, particularly as a security best practice. Second, when it is applied, segmentation is usually done to "reduce the scope of the assessment." It is often paired with the idea that "we don't have to secure the systems that aren't subject to review." The best thing to do is to segment your network to create security-defense-in-depth, not to limit scope, and apply the basic PCI DSS controls across the entire network.

Differences in levels

Companies often claim that "we are Level 1, 2, 3 or 4 PCI compliant" as if there is a different set of PCI DSS controls depending on the size of the company. This is a common misconception. The differences for the four merchant levels and the two service provider levels that the card brands recognize are in how a company validates annually that it is adhering to the PCI DSS. However, it is easy to understand the confusion, since smaller merchants and service providers are only required to self-assess and attest to their compliance using one of several Self-Assessment Questionnaires (SAQs) provided by the PCI SSC. The SAQs only provide what are believed to be the applicable requirements – based on the method of payment acceptance, or more simply how they merchant/service provider transmits, processes, or stores the data. So it would be easy to conclude that if you only have to validate against certain requirements, then those are the only requirements that apply. What is often missed is the disclaimer "you must still comply with all applicable PCI DSS requirements in order to be PCI DSS compliant." [3]

Audit of the year vs. business-as-usual

In the past, PCI DSS has emphasized the annual compliance requirement to the detriment of security compliance as a daily activity. Version 3.0 is now explicitly promoting a "business as usual" theme. While the idea of business as usual has been in PCI DSS in the past, it was not called out as a critical theme. In Version 3.0 it is receiving the coverage it deserves.

Self-assessment is not a solitary activity

The vast majority of Level 1 merchants do not retain a QSA; they go through a self-assessment questionnaire (SAQ), and they self-report on their PCI compliance. In fact, 99% of merchants report that they self-assess. There are now 9 versions of the Self-Assessment Questionnaire (SAQ) in Version 3.0 (up from 5 in the previous version). It can be very confusing to decide which questionnaire is appropriate for an organization, and it can be equally confusing to fill in a questionnaire accurately. Merchants may not read the entire standard or they may not fully understand what's involved in meeting a requirement. Fortunately, that is changing in Version 3; the Council has added a lot more detailed context into the self-assessment questionnaires.

Reliance on vendors may be risky

When an organization looks for a consultant to work through the PCI DSS requirements, the selected advisor is frequently a vendor who is also selling a security solution. It is important to separate his advice from the deployment, to decide if the consultant is right for your situation. And don't be fooled – most technology solutions have not met the PCI requirements for acceptance. Meeting the solutions associated with each requirement is important when validating the compliance of a company.

Low hanging fruit isn't as accessible

In the early days, the low hanging fruit for hackers were the millions of accounts stored in unencrypted database files, spreadsheets, flat files, log files for network devices, and notes. So during that time, PCI was all about cleanup,

finding out where all the data was stored, locating leaks, and placing data in secure containers, encrypted file systems or encrypted databases. The result was that capturing the data as it was swiped at the point of sale system seemed like a low return for hackers. But it quickly became a high return when they figured out how to steal data in an automated and efficient fashion. So today, the reality is that the landscape has changed; data in motion and data in process are hot commodities.

Credit card theft is still rampant

It is readily apparent from the many recent retail data breaches that credit card theft is still prevalent. Despite technology and hardened security policies, hackers are still staying one step ahead of merchants. This is why it is doubly important to adhere to the PCI DSS standards and to assure that you are adhering to the security requirements on a continuous or "business as usual" basis.

The network security landscape is changing

One of the biggest challenges to PCI DSS compliance is the changing network landscape. A PCI system could include desktops, laptops, smartphones, hand held scanners, virtual machines, cloud applications, and third party plugin applications. With traditional networks morphing into a perimeter-less system, security must also change. "Continuous monitoring" and "passive monitoring" become more important to meet the challenges of PCI DSS compliance.

Security Truths

If you only retain a few simple facts about PCI from this paper, remember these basic maxims:

Security is a verb

With the emphasis in DSS version 3.0 on business-as-usual, this one message should be abundantly clear: you have to practice security on an ongoing basis. Security is something that you do every day; it's a lifestyle, an attitude, a mindset. Security must permeate your employee base and your entire company. In short, security is a verb.

PCI compliance is an integral part of your security program

PCI DSS was designed to prevent the known and to provide the best possible framework to detect new events, to respond to them quickly, and to minimize the damage. One major section of the PCI DSS requirements ("Regularly Monitor and Test Networks") is devoted to making sure that you have logging enabled and that the logins are copied to a centralized source as a forensic trail[4]. A corresponding requirement talks about network time stamps so that you have forensic evidence for recreating an event, identifying the perpetrators, and prosecuting them. Those requirements wouldn't be there without the expectation that something bad is going to happen eventually.

So a real truth is that you should never separate PCI DSS from your entire security efforts. You might need to focus on specific areas more than others. But you shouldn't focus on trying to limit the scope of PCI DSS and sacrificing the big picture. PCI DSS doesn't discuss things you shouldn't do.

Attackers have advanced technologies

The technology and capabilities of the bad guys has advanced to the point where you really need this high level of protection. It's no longer a matter of hackers out there fishing for vulnerabilities; hackers have crafted targeted attacks that are highly successful against specific types of companies, operations and systems. It's almost inevitable that a hacker will find your business and attempt an intrusion. PCI conveniently gives you a solid security framework to meet the challenge.

You can pay now or you can pay later

Security comes with a price. Each of the PCI DSS requirements has different technologies and solutions associated with it, solutions that you must have in place to be compliant. Costs can involve:

- Hiring a QSA and/or an ASV
- Staff time to conduct testing and compliance
- Training, education, and awareness programs for staff who are responsible for CDE systems
- Implementing systems and solutions that are required to comply with specific standards

But are these investments costly? Relatively speaking, the costs are not that high. If you were hit with a data breach that resulted in stolen personal and/or credit card data, the cost of remediation could easily top $5.9 million[5]. Investing in PCI DSS compliance is like buying insurance – it may be an expense that a business doesn't want to pay, but in the long run, it is much less expensive and risky than the alternative of experiencing a catastrophic event.

So is it costly? Yes. Is it time consuming? Yes. Is it necessary? Yes.

Adjust your attitude

So what is the answer? Should we do away with PCI DSS and replace it with something better? Certainly the government is looking at the payment industry and trying to decide where to step in and legislate. But the problems do not stem from the standard itself, the problems are attitudinal: wanting to deal with PCI DSS as little as possible, to spend the least amount of money on PCI DSS, and to do the minimal amount of work to meet the requirements. Simply put, attitudes must be adjusted.

VI. How to make PCI work for you

If you're a stressed out by the reality of PCI DSS, that's good. You should be stressed out. But rather than panicking, you should be planning what to do.

Recommendations

PCI DSS may appear daunting, but taking it piece by piece, step by step, and integrating it into your larger security program, compliance should become routine. Integrate these basic recommendations into your security plans:

Embrace the PCI DSS

PCI DSS should be the framework for your security program. The overall framework has not changed since its inception, and it still holds up as a foundation for any solid security program. Technologies change, but the security fundamentals have not changed; the six original goals still apply to businesses today.

Choose the right QSA

Choosing the right QSA or Trusted Advisor can make all the difference in understanding and fully complying with the PCI DSS standards. Consider the costs of self-assessment in terms of time, personnel, and resources; a good QSA can save you time and headaches. The PCI maintains a list of certified QSAs, and VeriSign offers a paper on *Not All QSAs Are Created Equal: What You Should Know Before You Buy*.

Forget segmentation

PCI DSS does not require or recommend segmentation. Rather than trying to define and maintain segmented operations, take the high road and secure everything. Don't waste time, energy, and resources on limiting the scope of PCI compliance. Determine what you are not doing and implement those best practices for peace of mind.

Use PCI to justify security investments

While PCI can be costly to implement, the irony is that you can use PCI as a justification for getting what you need: security technologies, resources, and staff training programs.

Train your staff

It's not good enough to acquire and implement security technology – you must understand the tools and use them to their fullest potential. Your security analysis team must be properly trained and highly valued. Likewise, your employees should receive awareness training and understand their roles in maintaining security for the company. Security is everyone's job, not just the CISO's.

It's your responsibility

Even if you outsource, remember that it's your company's responsibility to secure customer data. Buying security technology alone does not make you secure. Security comes from deploying the products as part of a comprehensive security strategy, designed to minimize your risk.

Business as usual

How do you make PCI compliance an everyday task? First, all of the PCI DSS requirements should be applied as required — many requirements call for daily, weekly, or monthly validation activities to assure they are functioning appropriately. But in a larger sense, the PCI DSS needs to be treated as a framework for a security program (as it was originally intended) and applied to your organization as part of a regular and ongoing risk assessment process. Risk assessment requires that you understand the business needs, processes, and threats; you must know what sensitive data you have (that someone might want to steal); you should have a classification system for data with appropriate protection requirements; and you must document the processes for executing the plan. In short, you need to know your environment, know what needs to be protected, know how to do it, and execute.

Stay current

The PCI standards are dynamic; they will always be changing and updated as new threats, technologies, and processes emerge. For example, the success of EMV chip and PIN in Europe has led to it being mandated for adoption in the U.S. And it is still being rolled out globally; the U.S. is just one of the last major countries to adopt it. Realistically, it is going to take several years before EMV is completely adopted globally. When these target points become the most viable targets then we'll see attacks against these infrastructures. By staying current with PCI DSS, these attack points will be more secure and they won't get breached as often. PCI DSS will change as the technology changes; your security practices must be flexible and change, too. PCI DSS provides an overall security framework to protect PCI data now and in the future.

Security first, compliance second

If you take the "Security first, compliance second" approach, you might already be secure and compliant with PCI DSS requirements. Remember, security is an attitude, a mindset, a daily activity. When you live, breathe, and practice security, compliance becomes second nature. It doesn't mean that your business won't be in the news, but you stand a much better chance of avoiding a breach if you practice security for your entire network on a daily basis.

VII. How Tenable can help with security

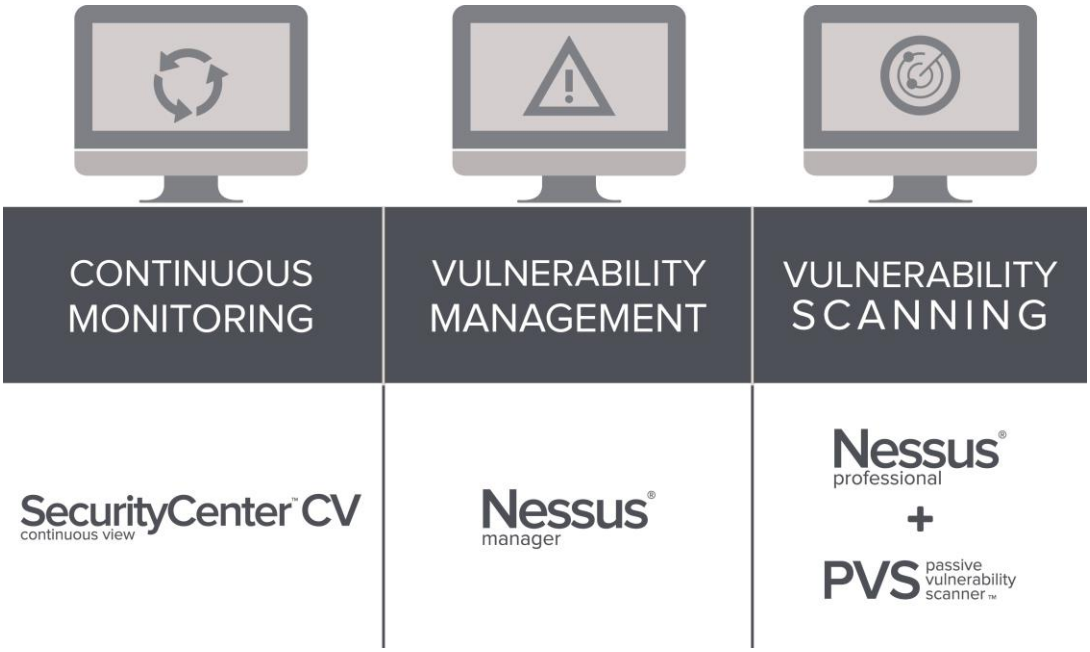
To ensure that security controls continue to be properly implemented, PCI DSS should be implemented into business-as-usual (BAU) activities as part of an organization's overall security strategy. Tenable products meet or exceed the best practices defined by the Council for integrating PCI DSS requirements into business-as-usual processes. This enables a business to monitor the effectiveness of their security controls on an ongoing basis, and maintain their PCI DSS compliant environment between annual PCI DSS assessments.

Tenable product portfolio

Tenable products can be divided into three categories:

- Continuous network monitoring
- Vulnerability management
- Vulnerability scanning

We emphasize continuous monitoring because that's where most companies must focus to be best positioned and secured in today's IT environment.



Nessus®: Meet PCI requirements

Tenable's Nessus® vulnerability scanner meets all PCI DSS internal scanning requirements. Nessus also tests web applications for secure coding to OWASP (Open Web Application Security Project, a virtual community that is dedicated to the security of web applications) specifications and performs web application vulnerability assessments.

Nessus can be used to:

- Baseline all in-scope systems for initial PCI compliance activities
- Perform configuration and compliance audits to determine whether systems are adhering to build standards, hardening guides, access controls, and user account management
- Determine if systems are current with anti-virus/anti-malware and patch protection

Nessus identifies sensitive data subject to PCI compliance requirements such as credit or debit primary account numbers. You can then identify and validate your cardholder data environment based on these results.

Nessus results can be used during a PCI compliance assessment to demonstrate that periodic and ongoing processes were maintained throughout the assessment period as required by numerous PCI DSS requirements.

Nessus Cloud: Meet ASV scan requirements

Tenable's Nessus Cloud provides quarterly external network scans to fulfill PCI external scanning requirements for all merchants and service providers. Nessus Cloud is a PCI-Certified Approved Scanning Vendor (ASV) solution.

Nessus Cloud may also be used to protect public-facing web applications by providing automated application vulnerability security assessments on a periodic basis or after any changes are made to the web application.

Tenable's PCI-certified professionals will review up to 2 PCI ASV scans per calendar quarter and, upon approval, will provide detailed and executive summary findings reports and the required Attestation of Compliance form.

PVS™: Enforce your cardholder data environment

The Passive Vulnerability Scanner™ (PVS™) provides continuous scanning of network security supported by pre-configured scanning scripts (plugins) and the ability to customize plugins for an organization's unique scanning requirements. Continuous scanning provides real-time analysis of the state of an organization's security. PVS is available as an individual product subscription or as an integrated component of SecurityCenter CV.

PVS detects internal data flows where cardholder data is involved. In particular, undocumented processes not included in the scoping of the cardholder data environment are readily identified.

PVS also detects unprotected transmissions of Primary Account Numbers (PANs) outbound from the network or cardholder data environment.

SecurityCenter CV™: Maintain ongoing compliance

Tenable's SecurityCenter Continuous View™ (SecurityCenter CV™) is the only comprehensive vulnerability, threat and compliance management platform that alleviates the arduous and time-consuming process of performing forensic analysis and threat or incident response. SecurityCenter CV secures your IT environment of physical and virtual systems as well as across mobile devices, virtual machines, and cloud services. SecurityCenter CV incorporates unlimited Nessus and PVS vulnerability scanners, and the Log Correlation Engine (LCE) in a SecurityCenter platform. Security Center CV offers large merchants continuous monitoring and centralized intelligence for maintaining an ongoing posture of compliance with the PCI standards.

SecurityCenter CV is used to:

- Continuously detect the presence of malware that infiltrated your network and is running malicious programs in your environment
- Monitor and discover new devices on the network that may impact the security of your cardholder data environment
- Identify PCI-relevant assets and focus vulnerability scans on those assets, reducing time and resources required for periodic scanning

SecurityCenter CV provides secure log normalization, aggregation, and storage. It facilitates the daily review of all logs. SC CV also enables the creation of a single view of risk exposure that includes Internet-facing web application vulnerabilities.

SecurityCenter CV is Tenable's optimum enterprise-class product for complying with PCI DSS.

Mapping Tenable solutions

In 2014, Tenable commissioned a report from CoalFire, a well-respected and independent IT governance, risk and compliance firm. CoalFire is credentialed as PCI SCC Approved Scanning Vendor and a PCI SSC Qualified Security Assessor Company. CoalFire evaluated our entire product suite, mapping PCI requirements to Tenable tools. The following summary table from the report[6] shows that SecurityCenter Continuous View meets 140 of the most important PCI DSS requirements.

PCI DSS Requirement	NUMBER OF PCI REQUIREMENTS	Nessus Cloud	Nessus Vulnerability Scanner	Passive Vulnerability scanner	Security Center Continuous view	Total Number of controls met or augmented by Tenable
Requirement 1: Install and maintain a firewall configuration to protect cardholder data	35		8	13	21	21
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	32		14	14	14	14
Requirement 3: Protect stored cardholder data	44		1	1	2	2
Requirement 4: Encrypt transmission of cardholder data across open, public networks	11	3	6	7	7	7
Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs	11		5	4	6	6
Requirement 6: Develop and maintain secure systems and applications	42	13	14	10	14	14
Requirement 7: Restrict access to cardholder data by business need to know	10		7		7	7
Requirement 8: Identify and authenticate access to system components	43		13		19	19
Requirement 9: Restrict physical access to cardholder data	44				1	1
Requirement 10: Track and monitor all access to network resources and cardholder data	41		3	2	23	23
Requirement 11: Regularly test security systems and processes	36	6	12	4	16	16
Requirement 12: Maintain a policy that addresses the information security for all personnel	47	2	2	5	8	8
Requirement A: Shared hosting providers must protect the cardholder data environment	8				2	2
TOTAL	404	30	85	60	140	140

Keep in mind that the PCI standard is roughly half technical requirements and half operational requirements. The technical requirements address systems that a QSA has to look at. The operational requirements are the ones that enumerate what you have written down. So Tenable products address approximately three quarters of the technical controls: 140 requirements out of approximately 200 technical controls, more than any other vendor.

VIII. Other Resources

For a comprehensive resource on all things PCI, visit the PCI Security Standards Council's website: www.pcisecuritystandards.org. The website provides all the PCI documentation, forms, questionnaires, and templates. It also offers compliance guidance, training opportunities, lists of QSAs and ASVs, webinars and other events.

Tenable hosts a discussion forum devoted to PCI called *Straight Talk about PCI*. This forum is a "safe" place where you can ask questions related to any and all aspects of PCI. The forum is intended to be a resource for accurate information about PCI DSS, particularly in the areas of defining terminology, scoping your cardholder data environment, properly navigating the compliance process, and providing interpretation, guidance, and advice on the best ways to satisfy the PCI compliance validation requirements faced by your organization.

IX. Terminology

AoC: Attestation of Compliance: The official signed document filled out by the assessed entity and the QSA which describes the scope of work and approach taken to assess the entity, provides a broad description of the type of payment card transactions processed, certain details of the CDE, and is signed by an officer of the assessed entity and the QSA of record (as applicable)

ASV: Approved Scanning Vendor: An organization that has been approved by the PCI SSC to validate adherence to the PCI DSS scan requirements by performing vulnerability scans of Internet-facing environments of merchants and service providers

CDE: Cardholder Data Environment: The people, processes and technology that store, process or transmit cardholder data or sensitive authentication data, including any connected system components

CDE: Cardholder Data Environment is the people, processes and technology that store, process, or transmit cardholder data or sensitive authentication data within a merchant and/or other third party's operations

CHD: Cardholder Data: Cardholder data minimally consists of the full Primary Account Number (PAN). CHD may also include cardholder name/address/phone number, expiration data, service code, sensitive authentication data, or magnetic stripe data.

PAN: Primary account number: The account number of a credit or debit card. This is a unique number that identifies the issuer and the cardholder account.

PCI: Payment Card Industry: The collective set of merchants and other entities that are involved in the transmission, processing, and/or storage of cardholder data throughout the payment card transaction and settlement process

PCI DSS: Payment Card Industry Data Security Standard: A basic guide to security best practices designed to protect cardholder data throughout the transaction and settlement process

PCI SSC: Payment Card Industry Security Standards Council: Administers the PCI DSS and other applicable standards that are used to protect cardholder data throughout the payment card transaction and settlement process

POI: Point Of Introduction: A device where a transaction starts when a credit card is swiped; a device on the counter or in the back room that someone uses to swipe a credit card or a debit card, with optional entry of a PIN by the customer

QSA: Qualified Security Assessor: An individual working for a QSA Company that is approved to assess compliance with the PCI DSS

RoC: Report on Compliance: The official mechanism by which merchants and other entities verify compliance with PCI DSS to their respective acquiring financial institutions (merchant banks) or to the payment card brands

SAD: Sensitive Authentication Data: Security information (such as card validation codes, track data, PINs, etc.) used in the authentication of cardholders and card transactions

SAQ: Self-Assessment Questionnaire: A validation tool for eligible organizations who self-assess their PCI DSS compliance and who are not required to submit a Report on Compliance

Track Data: Cardholder Data found on the Magnetic Stripe in multiple sections (or tracks) which generally includes all the information found embossed (or printed in the case of SAD) on the card

X. Endnotes

[1] PCI Security Standards Council, LLC. *Payment Card Industry (PCI) Data Security Standard: Requirements and Security Assessment Procedures Version 3.0*, November 2013, p. 5.

[2] *Ibid*, p. 13.

[3] PCI Security Standards Council, LLC. *Payment Card Industry (PCI) Data Security Standard: Self-Assessment Questionnaire A and Attestation of Compliance,* Version 3.0, February 2014, p. iii.

[4] *PCI DSS*, p. 82.

[5] PwC, *Global State of Information Security Survey 2015*, p. 10.

[6] CoalFire, *Tenable Addendum to VMware Product Applicability Guide for Payment Card Industry Data Security Standard (PCI DSS) version 3.0*, June 2014, p. 15.

XI. Bibliography

Coalfire. *Tenable Addendum to VMware Product Applicability Guide for Payment Card Industry Data Security Standard (PCI DSS), version 3.0*. June 2014. Available from: http://www.coalfire.com

PCI Security Standards Council, LLC. *Payment Card Industry (PCI) Data Security Standard: Requirements and Security Assessment Procedures*, Version 3.0. November 2013. Available from: https://www.pcisecuritystandards.org/security_standards/documents.php?agreements=pcidss&association=pcidss

PCI Security Standards Council, LLC. *Payment Card Industry (PCI) Data Security Standard: Self-Assessment Questionnaire A and Attestation of Compliance,* Version 3.0, February 2014. Available from: https://www.pcisecuritystandards.org/security_standards/documents.php

PwC. *Global State of Information Security Survey 2015*. Available from: http://www.pwc.com/gx/en/consulting-services/information-security-survey/

VeriSign. *Not All QSAs Are Created Equal: What You Should Know Before You Buy*. 2008. Available from: https://www.brandenwilliams.com/brwpubs/PCI_QSA_WP_051508.pdf

About Tenable Network Security

Tenable Network Security provides continuous network monitoring to identify vulnerabilities, reduce risk and ensure compliance. Our family of products includes SecurityCenter Continuous View™, which provides the most comprehensive and integrated view of network health, and Nessus®, the global standard in detecting and assessing network data. Tenable is relied upon by many of the world's largest corporations, not-for-profit organizations and public sector agencies, including the entire U.S. Department of Defense. For more information, please visit tenable.com.