Powerful Insights.
Proven Delivery.®

Thoughts on PCI DSS 3.0

September, 2014

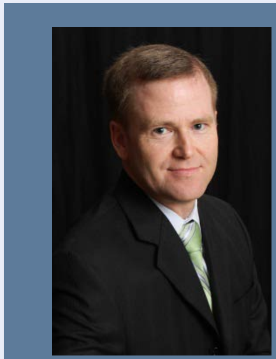
protiviti®
Risk & Business Consulting.
Internal Audit.

Speaker Today

Jeff Sanchez is a Managing Director in Protiviti's Los Angeles office. He joined Protiviti in 2002 after spending 10 years with Arthur Andersen's Technology Risk Consulting practice.

Jeff has participated in technical consulting and audit projects primarily in the hospitality, gaming, financial services and retail industries. Jeff leads Protiviti's global PCI practice and is a subject-matter expert in privacy and the Payment Card Industry Data Security Standard. For the last eight years, Jeff has concentrated on the design and implementation of security and privacy solutions. Jeff is a CIA, CISM, CISA, PA-QSA, CIPP/US and PMP.

jeffrey.sanchez@protiviti.com



Jeffrey Sanchez,
Managing Director

Agenda

1 *PCI DSS Overview*

2 *PCI DSS Version 3.0 Aims and Objectives*

3 *PCI DSS Version 3.0: Important Timelines*

5 *Scope of PCI DSS Requirements*

6 *End to End Encryption*

7 *PCI Data Security Standards Requirements*

8 *Questions*

PCI DSS Overview

The Payment Card Industry Data Security Standard (PCI DSS)

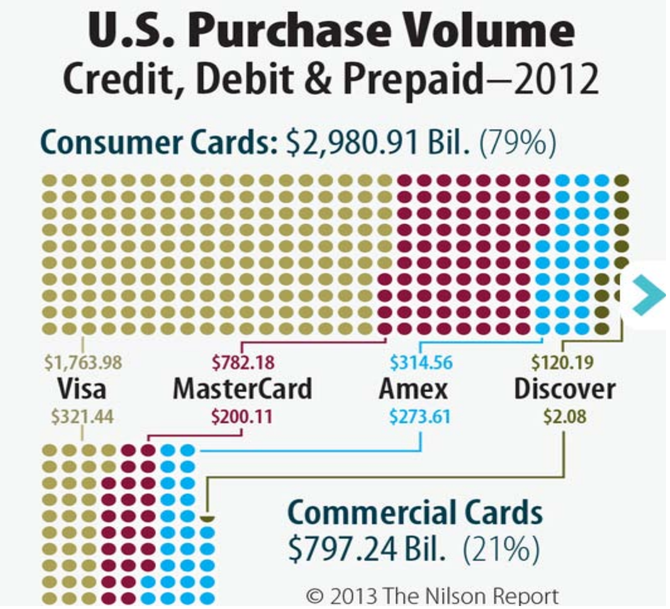
The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to ensure that **ALL** companies that **process, store** or **transmit** credit card information maintain a secure environment.

About PCI DSS

The PCI DSS is administered and managed by the PCI SSC, an independent body that was created by the major payment card brands (Visa, MasterCard, American Express, Discover and JCB.).

PCI applies to ALL organizations or merchants, regardless of size or number of transactions, that accept, transmit or store any cardholder data. Said another way, if any customer of that organization ever pays the merchant directly using a credit card or debit card, then the PCI DSS requirements apply.

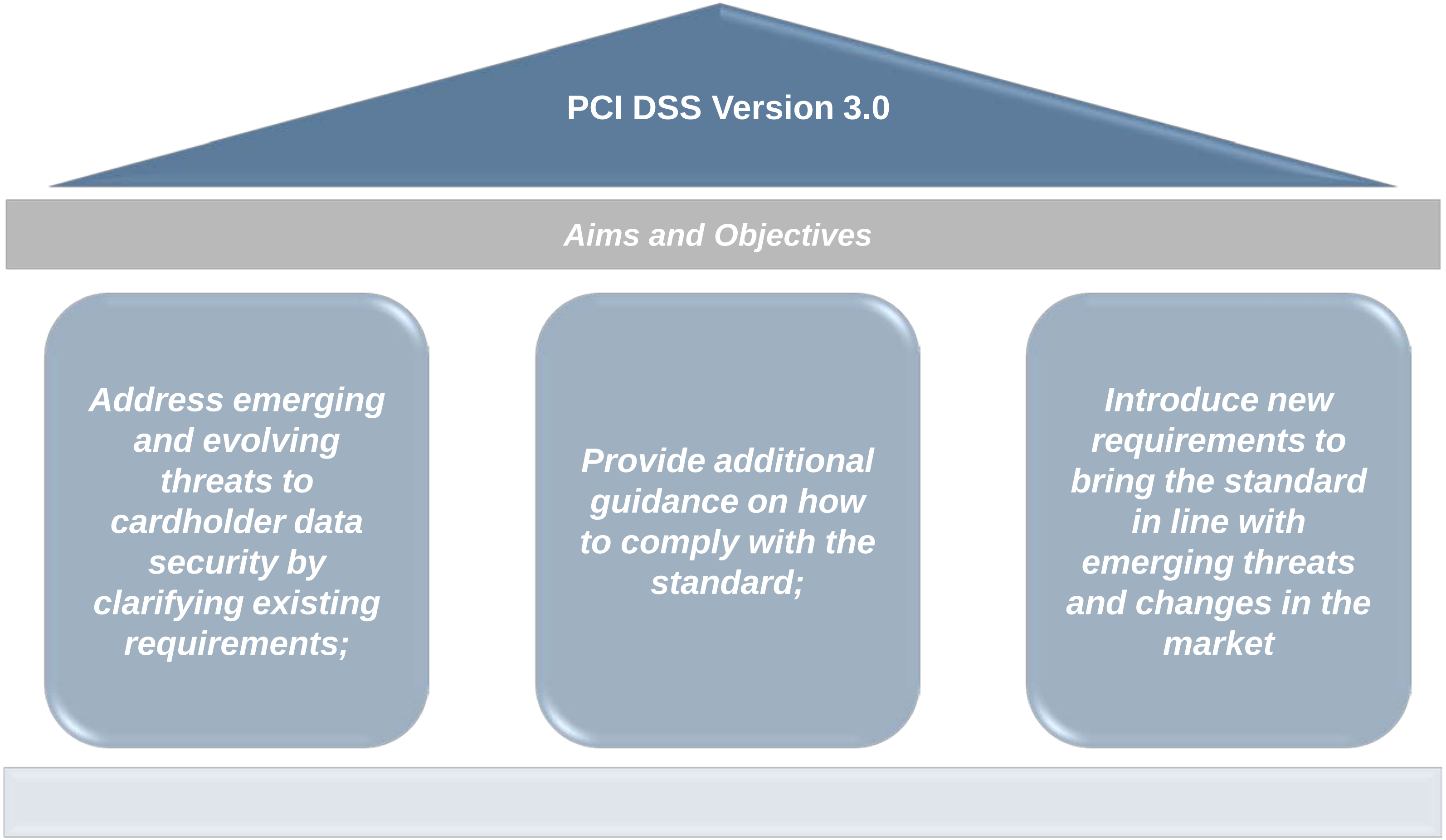
U.S. Purchase Volume - Consumer vs. Commercial Cards



Source: http://www.pcicomplianceguide.org/pcifaqs.php#2

PCI DSS Version 3.0 Aims and Objectives

Earlier this year, the PCI Security Standards Council (PCI SSC) announced the release of a new version of the PCI Data Security Standard (PCI DSS) Version 3.0. The new version aims to do the three things:



PCI DSS Version 3.0

Aims and Objectives

Address emerging and evolving threats to cardholder data security by clarifying existing requirements;

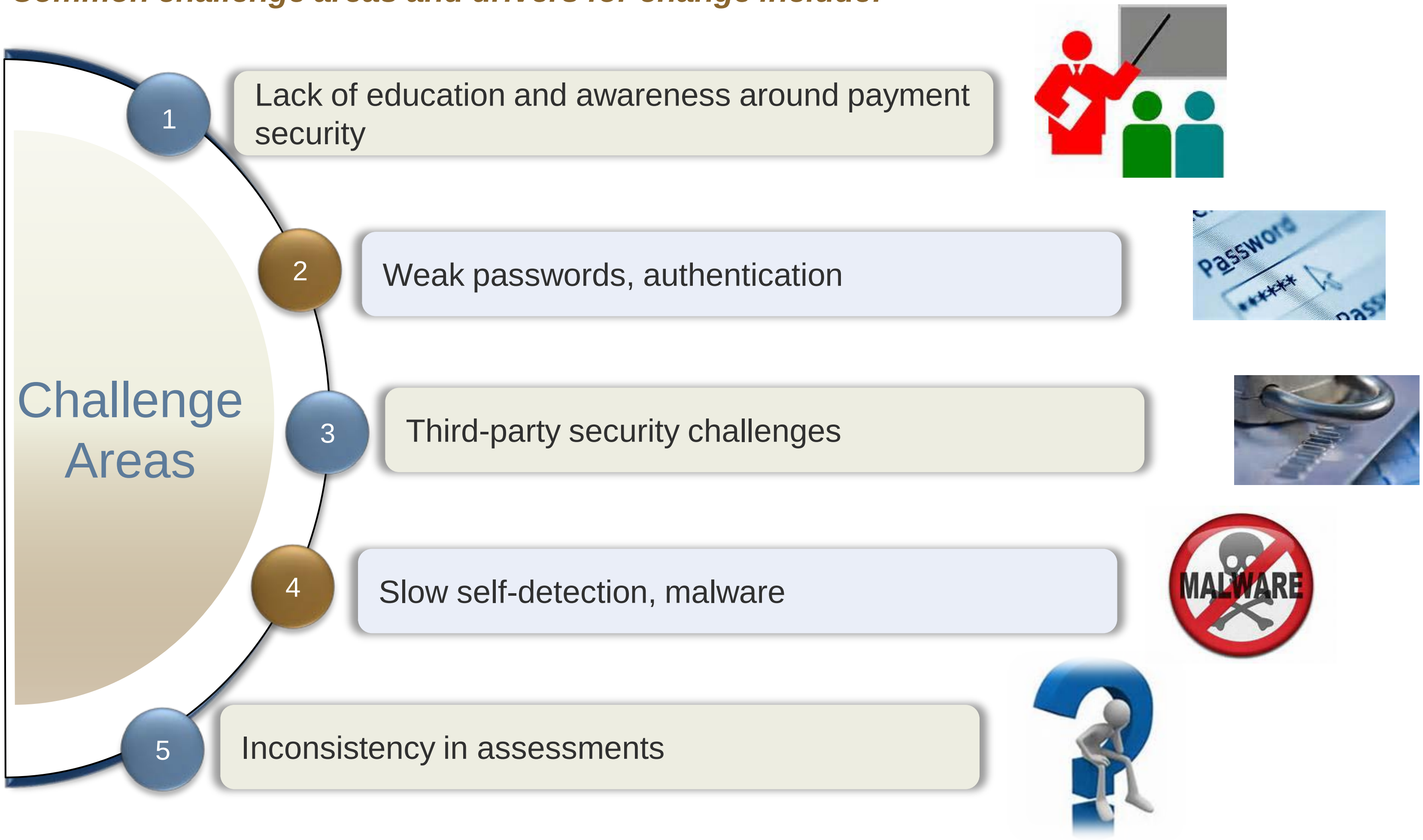
Provide additional guidance on how to comply with the standard;

Introduce new requirements to bring the standard in line with emerging threats and changes in the market

Source: ***INFORMATION TECHNOLOGY FLASH REPORT-Understanding PCI DSS Version 3.0 – Key Changes and New Requirements***

PCI DSS Version 3.0: Change Drivers

Common challenge areas and drivers for change include:



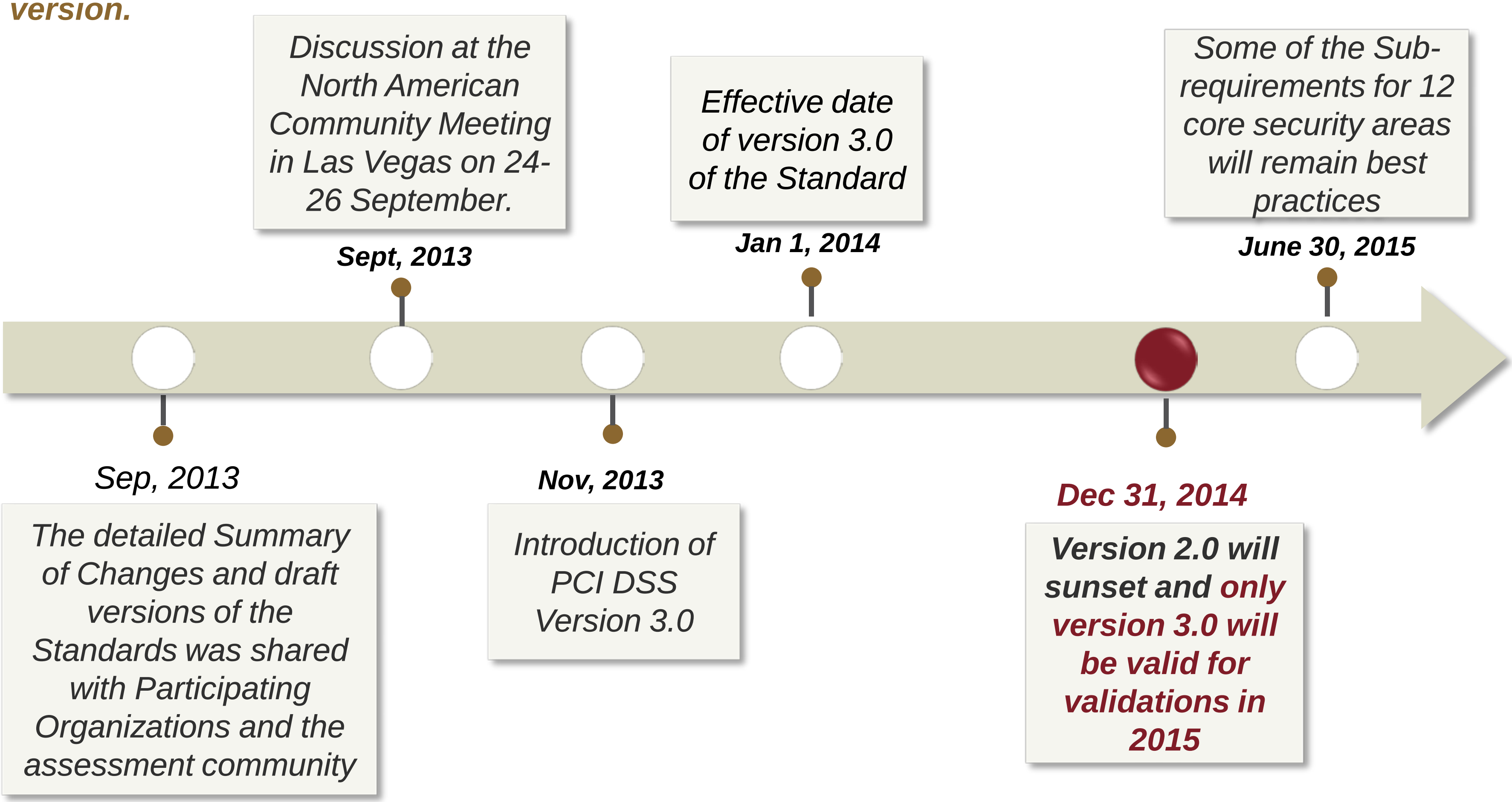
Challenge Areas

1. Lack of education and awareness around payment security
2. Weak passwords, authentication
3. Third-party security challenges
4. Slow self-detection, malware
5. Inconsistency in assessments

Source: *Data Security Standard and Payment Application Data Security Standard: Version 3.0 Change Highlights*

PCI DSS Version 3.0: Important Timelines

Recognizing that additional time may be necessary to implement some of these sub-requirements, the Council has given companies that process payment cards a full year to comply with the new standard. ***During 2014, both versions 2.0 and version 3.0 are available and companies can validate to either version.***



Sep, 2013

The detailed Summary of Changes and draft versions of the Standards was shared with Participating Organizations and the assessment community

Sept, 2013

Discussion at the North American Community Meeting in Las Vegas on 24-26 September.

Nov, 2013

Introduction of PCI DSS Version 3.0

Jan 1, 2014

Effective date of version 3.0 of the Standard

Dec 31, 2014

Version 2.0 will sunset and only version 3.0 will be valid for validations in 2015

June 30, 2015

Some of the Sub-requirements for 12 core security areas will remain best practices

Source: ***Data Security Standard and Payment Application Data Security Standard: Version 3.0 Change Highlights***

Scope of PCI DSS Requirements

Scope of PCI DSS Requirements

The PCI DSS security requirements apply to all system components included in or connected to the cardholder data environment (CDE). CDE is comprised of people, processes and technologies that store, process, or transmit cardholder data or sensitive authentication data.

System components include network devices, servers, computing devices, and applications. Examples of system components include:

- Systems that provide security services (for example, authentication servers), facilitate segmentation (for example, internal firewalls), or may impact the security of (for example, name resolution or web redirection servers) the CDE.
- Virtualization components such as virtual machines, virtual switches/routers, virtual appliances, virtual applications/desktops, and hypervisors.
- Network components including but not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances.
- Server types including but not limited to web, application, database, authentication, mail, proxy, Network Time Protocol (NTP), and Domain Name System (DNS).
- Applications including all purchased and custom applications, including internal and external (for example, Internet) applications.
- Any other component or device located within or connected to the CDE

Source: *PCI DSS Version 3.0- Requirements and Security Assessment Procedures*

PCI DSS Version 3.0: Most Notable Changes

Notable ☐ Most Notable ☑

A Higher Bar to Achieve "Segmentation"

- Specifically, scoping has been clarified to indicate that system components include, *"Any component or device located within or connected to the [cardholder data environment]."*

- The new language also states that the *"PCI DSS security requirements apply to all system components included in or connected to the cardholder data environment*

- Additionally, a new requirement has been added requiring that if segmentation is used, *"penetration testing procedures are designed to test all segmentation methods to confirm they are operational and effective, and isolate all out-of-scope systems from in-scope systems."*

- As further clarity, the standard states that*, "To be considered out of scope for PCI DSS, a system component must be properly isolated (segmented) from the CDE such that even if the out-of-scope system component was compromised it could not impact the security of the CDE."*

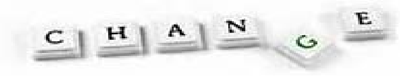
- The additional focus on connected systems likely expands (potentially greatly) the number of systems considered in-scope for many organizations. For example, in most networks using Windows Activity Directory security, a compromise of systems outside the CDE could impact the CDE and then could be considered in-scope for the PCI assessment.

Source: *INFORMATION TECHNOLOGY FLASH REPORT-Understanding PCI DSS Version 3.0 – Key Changes and New Requirements*

CONFIDENTIAL: This document is for your company's internal use only and may not be copied nor distributed to another third party.

PCI DSS Version 3.0: Most Notable Changes

Notable □ Most Notable ☑



Hosted Payment Pages Are No Longer A “silver bullet”

- PCI DSS 3.0 offers a new definition of system components: *“System components include systems that may impact the security of the CDE (for example web redirection servers).”*
- Up until now, web servers had been considered out-of-scope if they used iFrames, hosted payment pages or other redirection technologies to prevent cardholder data from touching the merchant’s systems.
- Under the new standard, all of these servers fall in-scope and, due to the new segmentation requirement, likely bring the rest of a company’s network into scope as well.
- The only “out” for companies that lack the ability to ensure the security of web servers internally remains fully outsourcing the web infrastructure.

Source: *INFORMATION TECHNOLOGY FLASH REPORT-Understanding PCI DSS Version 3.0 – Key Changes and New Requirements*

End to End Encryption

End-to-End Encryption

Becoming PCI compliant involves the use of advanced technology and tight security standards to keep customers' sensitive credit card data safe from fraud and security breaches. End-to-End Encryption (E2EE) is at the top of the list when it comes to emerging technologies that protect information and help merchants meet PCI requirements. PCI DSS 3.0 requires encrypting transmission of cardholder data across open, public networks.

- The rising cost of PCI DSS compliance and data breaches, and growing evidence that technology guidance from standards will not provide sufficient protection has led to a need for increased attention and education around end-to-end encryption and the role it should play in improving cardholder data security.
- Moreover, only by implementing end-to-end data protection throughout the entire payment ecosystem can the industry actually achieve the needed security for sensitive data. An example of this is how PIN data is protected in today's environment - from point of entry all the way to the issuer.

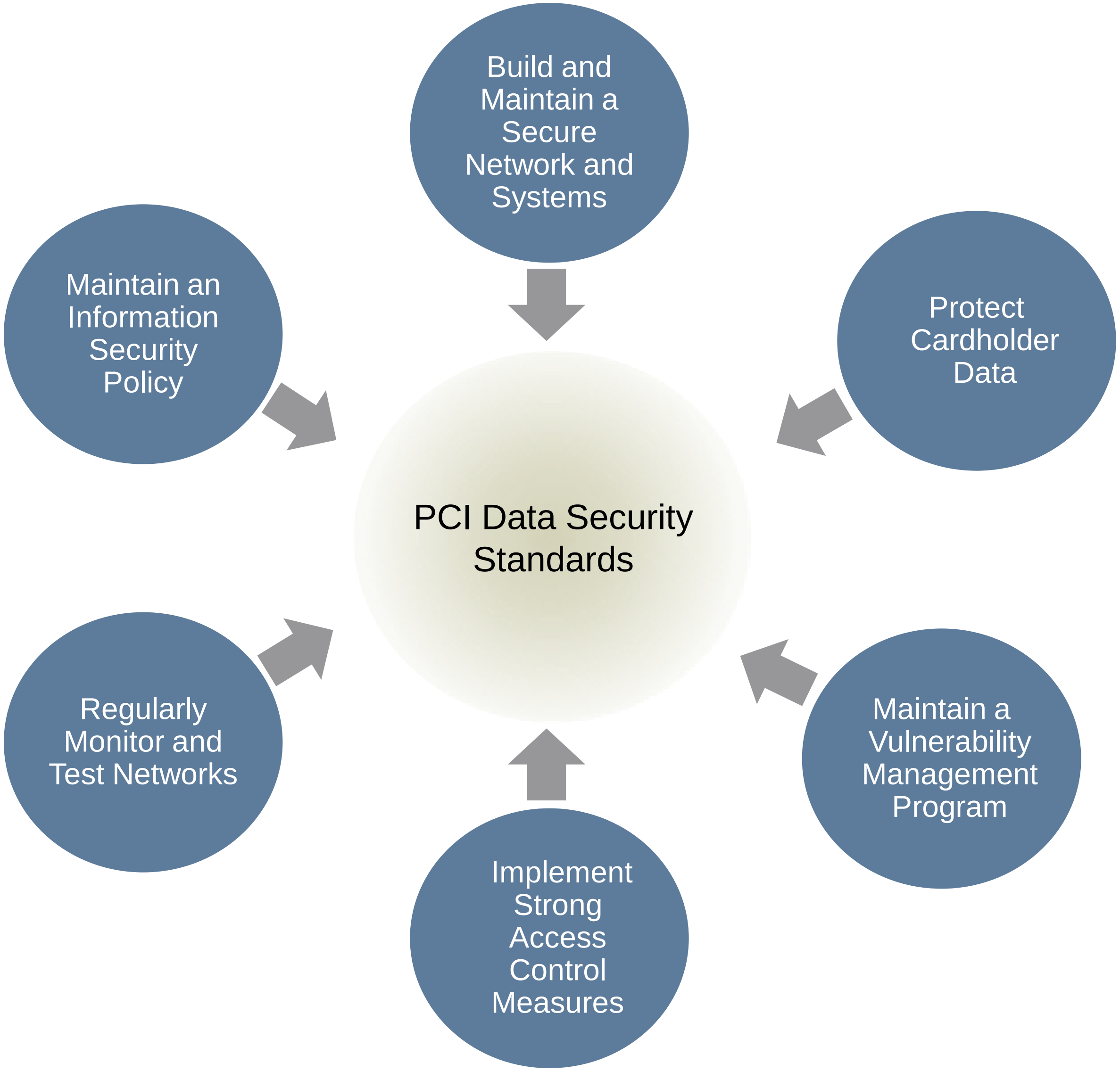
End-to-End Encryption

How does it work?

- State of the art encrypted magnetic card readers scan and encrypt cardholder information at first card swipe, prior to performing an electronic payment transaction.
- These devices securely encrypt cardholder data for transport over a network rendering it unreadable and as a result valueless to data thieves who frequently attempt to intercept the data while it is in transit to the processor.
- Each encrypted card reader is injected with an encryption key, unique to the processor, to allow for the decryption of the data once securely transmitted to the processor.
- Since these keys are unique and cannot be shared amongst processors, merchants are required to get new hardware when switching processing providers in order to continue to process transactions using end to end encryption.

PCI Data Security Standards Requirements

PCI Data Security Standards Requirements



Build and Maintain a Secure Network and Systems

Maintain an Information Security Policy

Protect Cardholder Data

PCI Data Security Standards

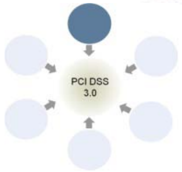
Regularly Monitor and Test Networks

Maintain a Vulnerability Management Program

Implement Strong Access Control Measures

Source: *PCI DSS Version 3.0- Requirements and Security Assessment Procedures*

Build and Maintain a Secure Network and Systems



Requirement 1: Install and maintain a firewall configuration to protect cardholder data

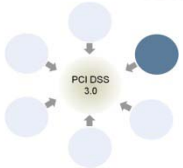
- Firewalls are devices that control computer traffic allowed between an entity’s networks (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within an entity’s internal trusted networks.
- A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.
- All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employee Internet access through desktop browsers, employee e-mail access, dedicated connections such as business-to-business connections, via wireless networks, or via other sources.
- Firewalls are a key protection mechanism for any computer network.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

- Malicious individuals (external and internal to an entity) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.
- Hence, always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network.
- Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.
- Enable only necessary services, protocols, daemons, etc., as required for the function of the system.

Source: *PCI DSS Version 3.0- Requirements and Security Assessment Procedures*

Protect Cardholder Data



***Requirement 3*: Protect stored cardholder data**

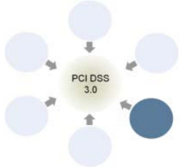
- Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person.
- For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending unprotected PANs using end-user messaging technologies, such as e-mail and instant messaging.
- Hence, it is important to not store sensitive authentication data after authorization (even if encrypted), card verification code or value, personal identification number (PIN). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process.

***Requirement 4:* Encrypt transmission of cardholder data across open, public networks**

- Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals.
- Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols continue to be targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments.
- It is recommended to use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks.

Source: *PCI DSS Version 3.0- Requirements and Security Assessment Procedures*

Maintain a Vulnerability Management Program



***Requirement 5*: Protect all systems against malware and regularly update anti-virus software or programs**

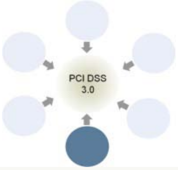
- Malicious software, commonly referred to as “malware”—including viruses, worms, and Trojans enters the network during many business-approved activities including employee e-mail and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities .
- Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats.
- Additional anti-malware solutions may be considered as a supplement to the anti-virus software; however, such additional solutions do not replace the need for anti-virus software to be in place.
- It is important to deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).
- Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.

***Requirement 6:* Develop and maintain secure systems and applications**

- Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches, which must be installed by the entities that manage the systems.
- All systems must have all appropriate software patches to protect against the exploitation and compromise of cardholder data by malicious individuals and malicious software.
- Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. It is important to install critical security patches within one month of release.

Source:* *PCI DSS Version 3.0- Requirements and Security Assessment Procedures

Implement Strong Access Control Measures



Requirement 7: ***Restrict access to cardholder data by business need to know***

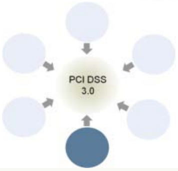
- To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities.
- Limit access should be given to system components and cardholder data to only those individuals whose job requires such access and assign access based on individual personnel’s job classification and function.
- It should be ensured that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.

Requirement 8: ***Identify and authenticate access to system components***

- Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for their actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users and processes.
- The effectiveness of a password is largely determined by the design and implementation of the authentication system—particularly, how frequently password attempts can be made by an attacker, and the security methods to protect user passwords at the point of entry, during transmission, and while in storage.
- Policies and procedures should be defined and implemented to ensure proper user identification management for non-consumer users and administrators on all system components.

Source: *PCI DSS Version 3.0- Requirements and Security Assessment Procedures*

Implement Strong Access Control Measures (Contd.)

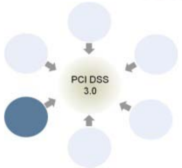


***Requirement 9:* Restrict physical access to cardholder data**

- Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted.
- For this requirement, “onsite personnel” refers to full-time and part-time employees, temporary employees, contractors and consultants who are physically present on the entity’s premises.
- A “visitor” refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day.
- “Media” refers to all paper and electronic media containing cardholder data.
- There should be procedures to easily distinguish between onsite personnel and visitors.

Source:* *PCI DSS Version 3.0- Requirements and Security Assessment Procedures

Regularly Monitor and Test Networks



Requirement 10: ***Track and monitor all access to network resources and cardholder data***

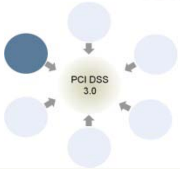
- Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong.
- Determining the cause of a compromise is very difficult without system activity logs.
- Therefore it becomes important to implement audit trails to link all access to system components to each individual user and retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).
- Logs and security events should be reviewed for all system components to identify anomalies or suspicious activity.

Requirement 11: ***Regularly test security systems and processes***

- Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software.
- System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.
- The organization should run internal and external network vulnerability scans at least quarterly and after any significant change in the network.

Source: *PCI DSS Version 3.0- Requirements and Security Assessment Procedures*

Maintain an Information Security Policy

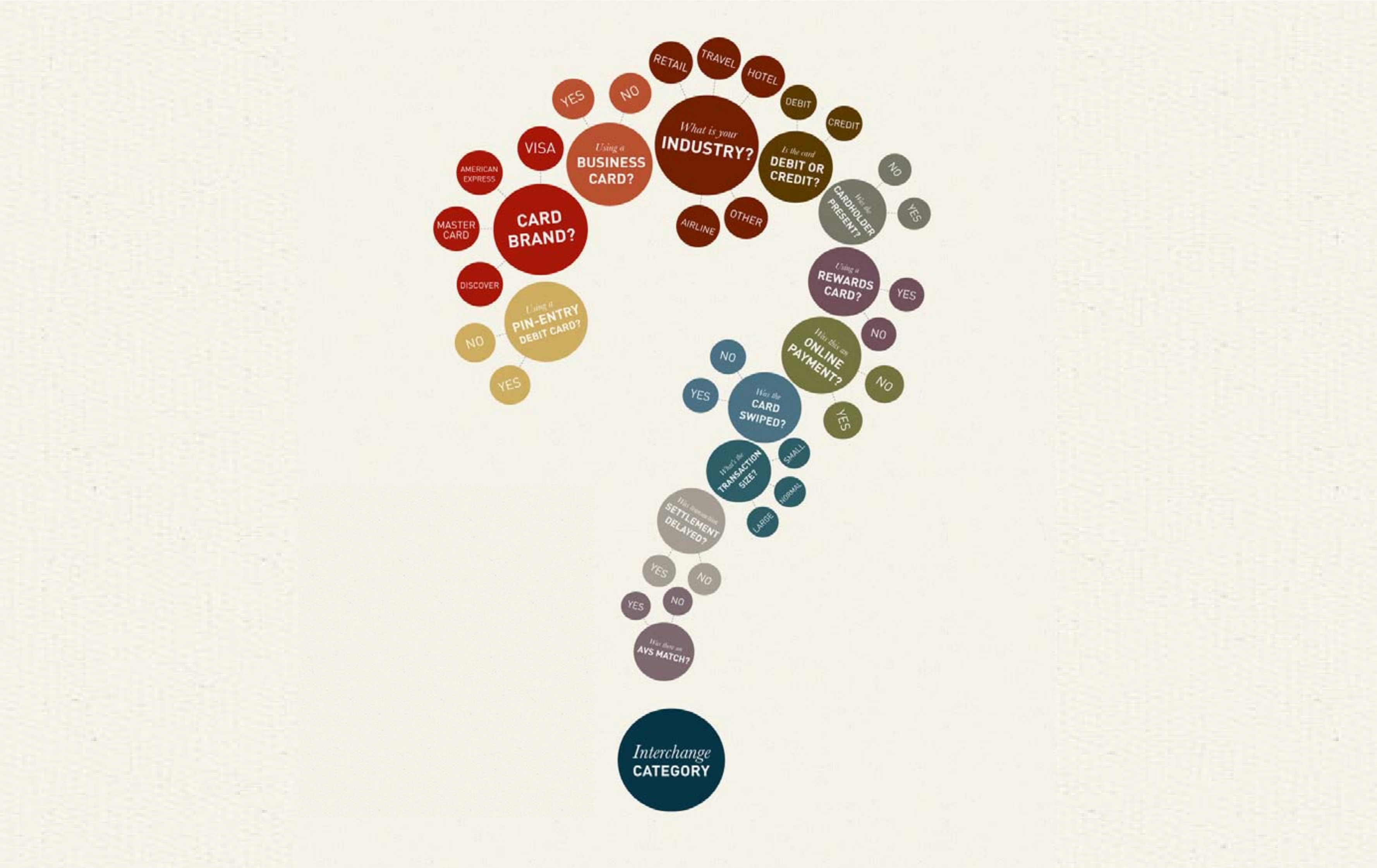


***Requirement 12:* Maintain a policy that addresses information security for all personnel**

- A strong security policy sets the security tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it.
- For this purpose “personnel” refers to full-time and part-time employees, temporary employees, contractors and consultants who are “resident” on the entity’s site or otherwise have access to the cardholder data environment.
- Ensure that the security policy and procedures clearly define information security responsibilities for all personnel; develop usage policies for critical technologies and define proper use of these technologies.

Source:* *PCI DSS Version 3.0- Requirements and Security Assessment Procedures

Questions



CONFIDENTIAL: This document is for your company's internal use only and may not be copied nor distributed to another third party.

Powerful Insights.
Proven Delivery.®

Confidentiality Statement and Restriction for Use

This document contains confidential material proprietary to Protiviti Inc. ("Protiviti"), a wholly-owned subsidiary of Robert Half ("RHI"). RHI is a publicly-traded company and as such, the materials, information, ideas, and concepts contained herein are non-public, should be used solely and exclusively to evaluate the capabilities of Protiviti to provide assistance to your Company, and should not be used in any inappropriate manner or in violation of applicable securities laws. The contents are intended for the use of your Company and may not be distributed to third parties.