



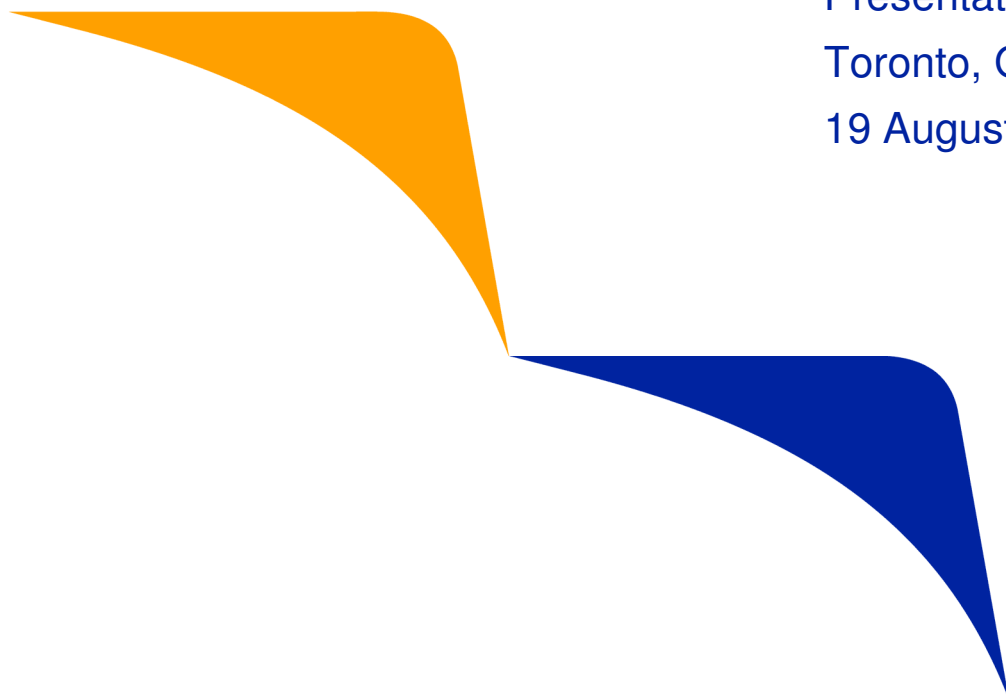
Will you be PCI DSS Compliant by September 2010?

Michael D'Sa, Visa Canada

Presentation to OWASP Toronto Chapter

Toronto, ON

19 August 2009



Security Environment

»» As PCI DSS compliance rates rise, new compromise trends emerge

Compliance Milestone

- PCI DSS compliance is adopted by acquiring participants in North America.
- Merchants and service providers reduce historical storage of cardholder data
- PCI DSS compliance improves among large merchants
- E-commerce and payment channel websites better secured



Compromise Trend

- Issuers and processors increasingly targeted; non-U.S. compromises increasing rapidly
- Data criminals seek capture of cardholder data in transit through sniffer attacks
- Compromises of small and medium size merchants increase
- SQL injection attacks on non-payment sites to gain access to payment environment

Compromises in the Media - Myths and Facts



Myths

- PCI DSS compliant entities have been breached
- PCI DSS does not address sniffer* attacks
- Visa does not support encryption
- Encryption of data transmission can prevent recent compromises



Facts

- As of today, no compromised entity has been found to be compliant at the time of the breach
- PCI DSS should prevent and detect unauthorized network access and installation of sniffers
- Visa does support encryption for both online and batch files
- Encryption does not eliminate the risk of data being “sniffed” if data is decrypted at any point



PCI DSS continues to serve as a robust foundation to protect cardholder data in a static data environment

*Sniffers are used by hackers to monitor and capture data in transit over an internal network

Common cyber vulnerabilities that lead to attacks on a network



Cyber Vulnerabilities



- No segmentation and/or firewall
- Un-patched systems and/or default configuration
- No logging
- No encryption or authentication on Wireless Access Points
- Security not written into payment applications
- Sniffer attacks
- Remote access misconfigurations

Forensic Findings*...



- The majority of all **E-commerce** merchant breaches are tied back to external hackers as opposed to insiders. On the other hand the number of “inside jobs” for **Brick/Mortar** data breaches still remains significantly higher.
- More than 80% of E-commerce merchant breaches could have been easily prevented if some basic security measures were in place.
- 20-25% of E-commerce merchant breaches were the result of SQL Injection – an attack that can be perpetrated quickly, easily and using any basic web browser from anywhere on the internet.
- Vulnerability Scanning is still critically important.
 - Some breached e-merchants were undergoing scans, but were not looking at their reports.
 - Some of these merchants were looking at the reports, but didn't bother to remediate the reported vulnerabilities.
 - Some of these reported vulnerabilities were known for over 12 months, but never addressed.

* Source: Verizon Business Powered by CyberTrust (2008)

Forensic Findings*...



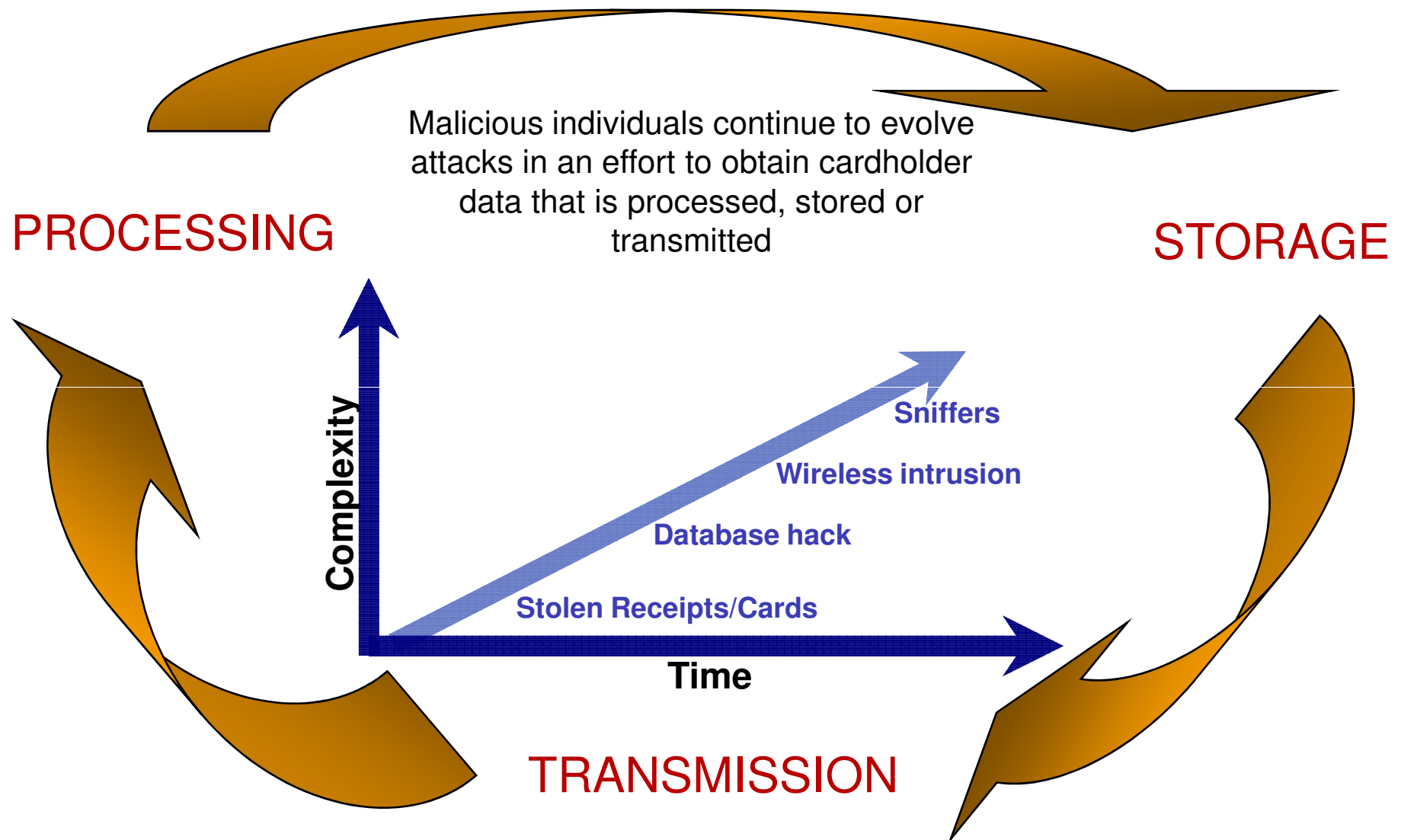
Approximately 50% of the E-commerce merchants' breaches tied back to issues with third parties.

These tend to fall into three sub-categories:

1. Outsourcing of the payment function (shopping cart check-out). The third party suffers a breach and the merchant's transaction data is compromised.
2. The e-commerce merchant sends transaction information to a third party, and permits the third party to connect into their e-commerce environment directly to pull the order fulfillment and transaction data. The third party suffers a compromise and the hacker exploits the connectivity that the third party has into the merchant to compromise the transaction data.
3. The shared hosting provider scenario. Many e-commerce sites are being hosted in shared environments. In these shared scenarios there is little to no segmentation between the various e-commerce sites that may exist in the shared environment. One merchant or entity that is hosted in the environment can suffer a breach and then the hacker gains access to the database – which can contain transaction information for dozens or even hundreds of merchants.

* Source: Verizon Business Powered by CyberTrust (2008)

What Are We Up Against?



Compromise Event Impacts



When Cardholder Data is Compromised

Compromised Entity

1. Financial Liability
 - Fines
 - Cost of forensic exam
 - Fraud Liability
2. Brand/Reputation Damage
3. Disruption of Service

Visa's Data Security Program



Account Information Security

is a Visa **mandated** program that outlines the minimum level of security for any entity that transmits, processes, or stores Visa account information.

The AIS program utilizes the **PCI Data Security Standard** and related suite of documents.



Compliance Validation Summary – Merchants



1

2





3

4

Annual Visa Transaction Volume	Merchant Type	Self-Assessment Questionnaire	Vulnerability Scan	On-site Review
over 6,000,000	All		✓ Quarterly	✓ Annual
1,000,000 to 6,000,000	All	✓ Annual	✓ Quarterly	
20,000 to 1,000,000	E-commerce Volume	✓ Annual	✓ Quarterly	
B/M and MOTO < 1,000,000 E-comm < 20,000	All other merchants	✓ Annual	✓ Annual	

Compliance Validation Summary – Service Providers



	Service Provider Type	Self-Assessment Questionnaire	Vulnerability Scan	On-site Review
1	VisaNet processors or any service provider that stores, processes and/or transmits over 300,000 transactions per year		 Quarterly	 Annual
2	Any service provider that stores, processes and/or transmits less than 300,000 transactions per year	 Annual	 Quarterly	

Deadlines



- Level 1, 2, and 3 merchants were required to complete their validation compliance review by 31 December 2005.
- Visa Canada agreed not to levy fines if a merchant had a reasonable action plan in place
- Visa Inc announced a global date (September 30, 2010), which enforces fines on L1 merchants who have not completed their DSS validation reviews
- Fines will be levied to the respective Acquirers of non-compliant L1 merchants after September 30, 2010
- Visa Canada will announce an end date for L2 and L3 merchants

PCI Training in Canada



PCI DSS 1.2 Training
Location: Toronto
June 16, 17

PCI PA-DSS Training
Location: Toronto
June 18

PCI DSS 1.2 Training
Location: Vancouver
September 9/10



PCI DSS Prioritized Approach



What is the Prioritized Approach?

The Prioritized Approach is a new educational resource from the Council. It offers guidance on how to focus PCI DSS implementation efforts in a way that expedites the security of cardholder data.



PCI DSS Prioritized Approach



How can the Prioritized Approach help with compliance?

The Prioritized Approach does not provide a short cut or tricks to achieve PCI DSS compliance. It does however deliver key benefits, such as:

- Helps businesses identify highest risk targets
- Creates a common language around PCI DSS implementation efforts
- Enables merchants to demonstrate progress on compliance process to key stakeholders – banks, acquirers, QSAs, others.

PCI DSS Prioritized Approach



How was it created?

- Examination of account data compromise events
- Feedback from PCI SSC Board of Advisors, Council leadership and the Technical Working Group
- Feedback from several QSAs and forensics investigators
 - *Asked to identify the top 15 PCI DSS requirements for protecting cardholder data*

Reduce risk associated with account data compromise by:

- Not retaining magnetic stripe data
- Minimize and secure storage of PAN
- Using network segmentation to reduce scope

PCI DSS Prioritized Approach



Milestone One - If you don't need it, don't store it.

The intent of Milestone One is to remove sensitive authentication data and limit data retention. This milestone targets a key area of risk for entities that have been compromised – if sensitive authentication data and other cardholder data had not been stored, the effects of the compromise would have been greatly reduced.

Milestone Two - Secure the perimeter.

The intent of Milestone Two is to protect the perimeter, internal, and wireless networks. This milestone targets a key area that represents the point of access for most compromises: vulnerabilities in networks or at wireless access points.

PCI DSS Prioritized Approach



Milestone Three - Secure applications.

The intent of Milestone Three is to secure applications. This milestone focuses on applications, as well as application processes and application servers, since application weaknesses are a key access point used to compromise systems and obtain access to cardholder data.

Milestone Four - Control access to your systems.

The intent of Milestone Four is to protect the cardholder data environment through monitoring and access control since this is the key method to detect the who, what, when and how about who is accessing your network.

PCI DSS Prioritized Approach



Milestone Five - Protect stored cardholder data.

For those organizations that have analyzed their business processes and determined that they must store Primary Account Numbers, Milestone Five targets key protection mechanisms for that stored data.

Milestone Six - Finalize remaining compliance efforts, and ensure all controls are in place.

The intent of Milestone Six is to complete PCI DSS requirements and finalize all remaining related policies, procedures, and processes needed to protect the cardholder data environment.

PCI DSS Prioritized Approach



PCI COMPLIANCE IS A CONTINUOUS PROCESS

PCI SSC FOUNDERS

PARTICIPATING ORGANIZATIONS

Merchants, banks, processors, developers and point of sale vendors

PCI DSS PRIORITIZED APPROACH

Disclaimer

To achieve PCI DSS compliance, an organization must meet all PCI DSS requirements, regardless of the order in which they are satisfied or whether the organization seeking compliance follows the PCI DSS Prioritized Approach. This document does not modify or abridge the PCI DSS or any of its requirements, and may be changed without notice. PCI SSC is not responsible for errors or damages of any kind resulting from the use of the information contained herein. PCI SSC makes no warranty, guarantee, or representation as to the accuracy or sufficiency of the information provided herein, and assumes no responsibility or liability regarding the use or misuse of such information.

Milestones for Prioritizing PCI DSS Compliance Efforts

The Prioritized Approach includes six milestones. The matrix below summarizes high-level goals and intentions of each milestone. The rest of this document details milestones to each of all twelve PCI DSS requirements and their sub-requirements.

Milestone	Goals
1	Remove sensitive authentication data and limit data retention. This milestone targets a key area of risk for entities that have been compromised. Remember – if sensitive authentication data and other cardholder data are stored, the effects of a compromise will be greatly reduced. If you don't store it, it, don't store it.
2	Protect the perimeter, internal, and wireless networks. This milestone targets controls for points of access to most compromises – the wireless access point.
3	Secure payment card applications. This milestone targets controls for applications, application processes, and application servers. Web services and these areas offer easy prey for compromising systems and obtaining cardholder data.
4	Monitor and control access to your systems. Controls for this milestone allow you to detect the who, what, when, and how concerning who is accessing your network and cardholder data environment.
5	Protect stored cardholder data. For those organizations that have analyzed their business processes and determined that they must store Primary Account Numbers, Milestone Five targets key protection mechanisms for that stored data.
6	Finalize all policies, procedures, and processes to support maintenance of PCI DSS compliance. The intent of Milestone 6 is to complete PCI DSS requirements, and to finalize all remaining related policies, procedures, and processes needed to protect the cardholder data environment. The milestone also includes completion of firewall configuration standards, change control procedures, securing audit trails, and network testing processes.

Prioritized Approach Tools

PCI DSS Requirements		Milestone					
		1	2	3	4	5	6
Requirement 1: Install and maintain a firewall configuration to protect cardholder data							
1.1	Establish firewall and router configuration standards that include the following:						6
1.1.1	A formal process for approving and testing all network connections and changes to the firewall and router configurations						
1.1.2	Current network diagram with all connections to cardholder data, including any wireless networks	1					
1.1.3	Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone		2				
1.1.4	Description of groups, roles, and responsibilities for logical management of network components						6
1.1.5	Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure		2				
1.1.6	Requirement to review firewall and router rule sets at least every six months						6
1.2	Build a firewall configuration that restricts connections between untrusted networks and any system components in the cardholder data environment.		2				
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.						

PCI DSS Prioritized Approach



The Prioritized Approach does not

- Provide a short cut to compliance with PCI DSS 1.2
- Assume a one size fits all approach for every organization
- Replace PCI DSS 1.2

PCI DSS Prioritized Approach



The use of the Prioritized Approach is not mandated

- QSAs are not obliged to use this approach for reporting purposes, but encouraged to become familiar with the approach
- Merchants and Service Providers are still required to be fully compliant with PCI DSS
- Safe Harbour only afforded to entities that are fully compliant

For more details on the Prioritized Approach, please refer to the PCI Security Standards website, **www.pcisecuritystandards.org**

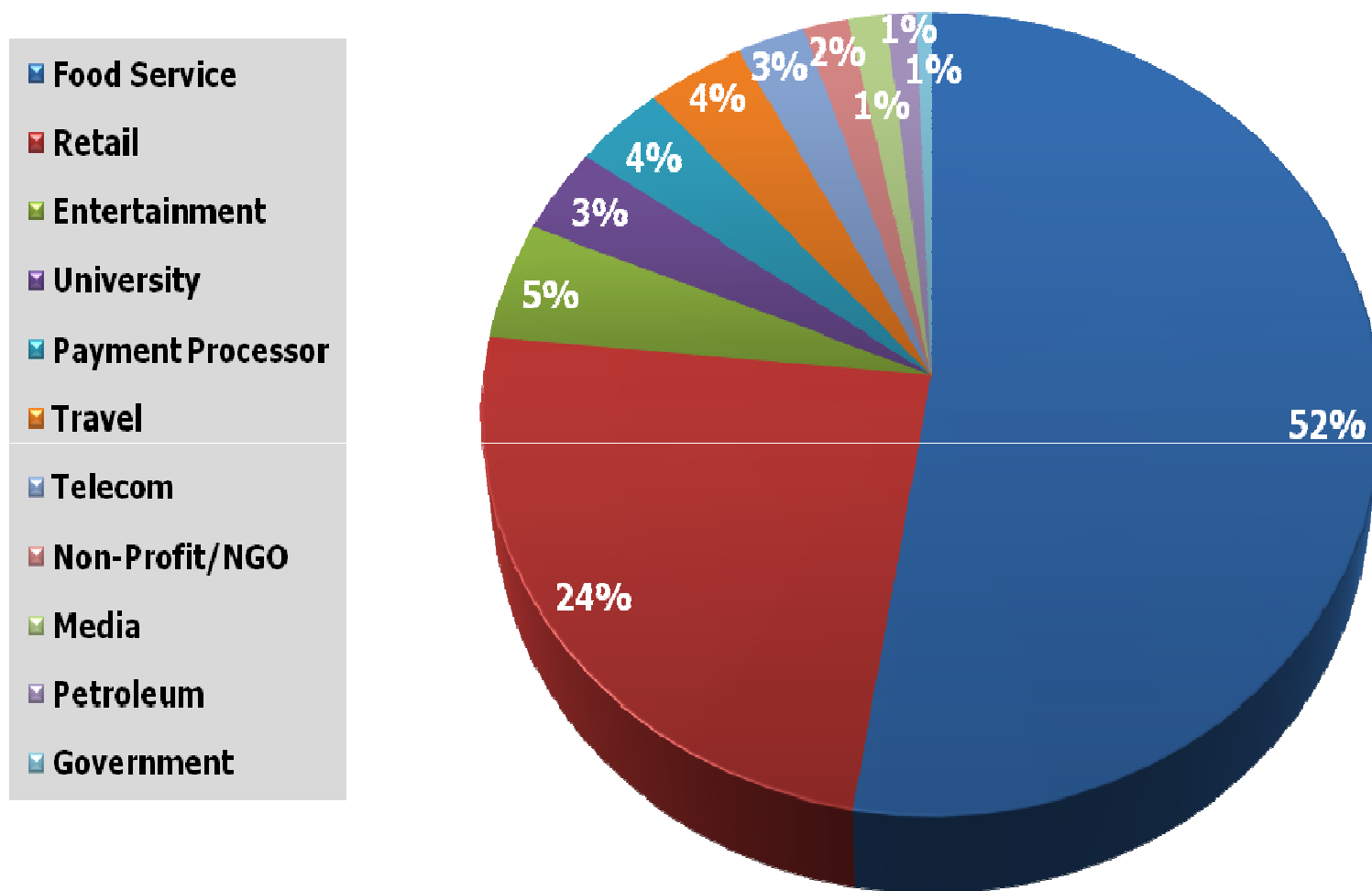


Payment Application Compliance Program

A Program Overview



Compromise Incidents by Industry



*Source: TrustWave, 2008

What is the PA-DSS?



- PA-DSS is a comprehensive set of security requirements designed for payment application software vendors to facilitate their customers' PCI DSS compliance
- This comprehensive standard is intended to help organizations minimize the potential for security breaches due to flawed payment applications, leading to compromise of sensitive authentication data
- Distinct from, but aligned with PCI DSS

Payment Application Data Security Standard



1. Do not retain full magnetic stripe, CVV2, or PIN block data.
2. Protect stored cardholder data.
3. Provide secure password features.
4. Log application activity.
5. Develop secure applications.
6. Protect wireless transmissions.
7. Test applications to address vulnerabilities.
8. Facilitate secure network implementation.
9. Cardholder data must never be stored on a server connected to the Internet.
10. Facilitate secure remote software updates.
11. Facilitate secure remote access to application.
12. Encrypt sensitive traffic over public networks.
13. Encrypt all non-console administrative access.
14. Develop, maintain and disseminate a PABP implementation guide for customers, resellers and integrators.

Payment Application Vulnerabilities



Over 24 applications have played a role in data compromises*

Top 5 vulnerabilities related to payment applications include:

- SQL injection
- Default accounts
- Full track data and/or encrypted PIN block retention
- Insecure remote access by software vendors and their resellers
- Compatibility issues with anti-virus and encryption

*Source: Visa Inc. Payment System Risk, 2007

Important Dates – Visa Canada



- Effective **October 1, 2008**, Visa Canada requires all newly boarded merchants who use Payment Application software to use software that has been validated to comply with PA-DSS
- Effective **July 1, 2010**, all existing merchants who use Payment Application software must use software that has been validated to comply with PA-DSS

PCI Security Standards Council



- The PCI Security Standards Council (PCI SSC) is an open global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection.
- Its mission is to enhance payment account security by fostering broad adoption of PCI Security Standards.
- The founding members are Visa, Amex, Discover, JCB and MasterCard.

Participating Organizations



Participating Organizations contribute to PCI SSC by:

- Providing advance comment on potential changes to security standards
- Providing input on future initiatives of the organization
- Nominating representatives for election to the Advisory Board
- Providing strategic direction to the organization by serving on the Advisory Board

www. PCISecurityStandards.org



Home - PCI Security Standards Council - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://www.pcisecuritystandards.org/

Google

PCI Security Standards Council

Site Map Contact Us Privacy Policy Terms & Conditions

Search

Security Standards QSA/ASV Participation Education News & Events About Us

Join Now

FAQ

Resources for Merchants & Service Providers

Career Opportunities

QUICK LINKS

Get the PCI DSS

Get the DSS Self-Assessment Questionnaire (SAQ)

Get the PIN Entry Devices (PED)

Get the Payment Application DSS (PA-DSS)

Find a QSA or an ASV

Become a QSA

Become a PA-QSA

Become an ASV

Submit QSA Feedback Form

Submit ASV Feedback Form

Welcome to the
PCI Security Standards Council

The PCI Security Standards Council is an open global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection.

The PCI Security Standards Council's mission is to enhance payment account data security by driving education and awareness of the PCI Security Standards. The organization was founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa, Inc.

PCI Data Security Standard 1.2 released October 1, 2008. [Read More](#)

View **PCI Quick Reference Guide**

PCI Data Security Standard

The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures.

[Read More](#)

PIN Entry Device (PED) Standard

The Payment Card Industry (PCI) has initiated a collaborative effort to address common industry security criteria.

[Read More](#)

PCI SSC – Visa Inc.’s 2009 Objectives



As a founding member, Visa drives key industry data security initiatives through the PSI SSC

- **Perform QSA quality assurance reviews**
- **Formal publication of a risk-prioritization strategy**
 - Visa to develop corresponding qualification criteria for entities to validate using risk-prioritization
- **Adoption and publication of PCI PIN Security Standard**
- **Determine feasibility for Council’s management of Forensic Investigators program**
- **Development of card issuer guidance for PCI DSS compliance**

Conclusion



Too much emphasis on PCI DSS validation as a finish line rather than ongoing security and compliance leaves exposure

- PCI DSS controls, when implemented properly, would prevent network intrusions
 - If the network is compromised, impact should be mitigated via timely detection
- In all compromise cases, forensic investigations have found significant gaps in the compromised entity's PCI DSS controls to be major contributors to the breach
- Validating compliance is a snapshot, point-in-time review of a business' systems, and is limited in scope to a sample of systems
 - Entities must not rely solely on a Qualified Security Assessors to determine their compliance
- Maintaining good security requires an ongoing commitment
 - PCI DSS compliance is a 24 hour a day, 7 day a week, 365 day a year job
 - Businesses must build ongoing compliance monitoring into their internal auditing processes

