



Confidence in a connected world.



Payment Card Industry Data Security Standard

Mark Lewis CISSP, CISA

Sr. Systems Engineer, Channels

October 21st, 2008

1 Introduction

2 What is PCI?

3 Consequences of Non-Compliance

4 How Symantec can Help

5 Conclusion



Confidence in a connected world.

Introduction

Why a standard for payment cards?



- Credit card companies and banks have for years absorbed the losses associated with fraud – and passed it on to the consumer in the form of higher interest rates and costs
- This has ended – especially with the realization that simple losses to merchants are multiplying with the costs associated with identity theft which can be much greater than the costs of goods obtained by fraud
- They want the parties associated with creating the risk to absorb the costs associated with poor information handling practices



Confidence in a connected world.

What is PCI?

- Most major credit card companies have adopted the Payment Card Industry (PCI) Data Security Standard, which was jointly developed by VISA and MasterCard
- Adopters of the standard include American Express, Diners Club, Discover, and JCB International
- All merchants and service providers that store, process, or transmit cardholder data **MUST** comply with PCI-DSS
 - applies to all payment channels (such as retail, mail/telephone order, e-commerce)
- Escalates requirements for firms based on transaction counts and other risk factors

Audience: Who does this impact?



- Retailers, obviously
- But also:
 - Utilities and telecom
 - Government
 - Financial (insurance)
 - Oil and Gas
 - E-commerce sites
 - Banks, as well, must comply
- About 75% of companies receiving payments by credit card are still moving towards or have done nothing about PCI compliance – a wide open area for risk

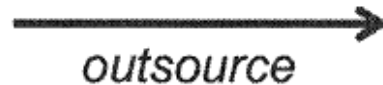
Organizations that store, process or transmit cardholder data:

- **Merchants**
 - Organizations of all sizes
 - Recognized and segmented by card transaction volumes
- **Service Providers**
 - Third-party processors in the payment system
 - Payment gateways
 - Recognized and segmented by card transaction volumes
- **Payment Software Providers**
 - Vendors of payment applications
 - Market share and risk profile not currently tracked

Who's Who for Payment Card Transactions: Merchants, Acquirers, and Issuers



Who's Who for Payment Card Transactions: Service Providers and Payment Gateways



- Stores, processes, and/or transmits cardholder data as part of payment transaction
- Enables transactions between merchants and processors

Merchant Segments Defined By Risk Priority



Level 1	<p>Any merchant-regardless of acceptance channel-processing over 6,000,000 Visa or Mastercard transactions per year.</p> <p>Any merchant that has suffered a hack or an attack that resulted in an account data compromise.</p> <p>Any merchant that Visa or Mastercard, at its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the Visa or Mastercard system.</p> <p>Any merchant identified by any other payment card brand as Level 1.</p>
Level 2	<p>Any merchant processing 1 million to 6 million Visa or MasterCard transactions per year</p>
Level 3	<p>Any merchant processing 20 thousand to 1 million Visa or MasterCard e-commerce transactions per year</p>
Level 4	<p>Any merchant processing less than 20 thousand Visa or MasterCard e-commerce transactions per year, and all other merchants processing up to 1 million Visa transactions per year</p>

Note: Annual Transaction Volume is based on DBA, or chain

Source: http://usa.visa.com/business/accepting_visas_ops_risk_management/cisp.html

Service Provider Segments Defined By Risk Priority



Level 1	<ul style="list-style-type: none">• All VisaNet processors, both Member and non-member• Service providers that store, process, and/or transit > 1 million Visa accounts/transactions annually• All compromised service providers• Service provided identified as Level 1 by another payment brand
Level 2	<ul style="list-style-type: none">• Any service provider that is not in Level 1 and stores, processes, or transmits more than 1 million Visa accounts/transactions annually
Level 3	<ul style="list-style-type: none">• Any service provider that is not in Level 1 and stores, processes, or transmits less than 1 million Visa accounts/transactions annually

Note: proposed is only Level 1 and Level 2 Service Providers
Source: http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html

Merchant Level



Level	Validation Action	Validated By	Due Date
1	Annual On-site PCI Data Security Assessment And Quarterly Network Scan	-Qualified Security Assessor or Internal Audit if signed by Officer of the company -Approved Scanning Vendor	9/30/04 New level 1 merchants have up to one year from identification to validate.
2	Annual PCI Self-Assessment Questionnaire and Quarterly Network Scan	-Merchant -Approved Scanning Vendor	New level 2 merchants: 9/30/2007
3	Annual PCI Self-Assessment Questionnaire and Quarterly Network Scan	-Merchant -Approved Scanning Vendor	6/30/05
4*	Annual PCI Self-Assessment Questionnaire and Quarterly Network Scan	-Merchant -Approved Scanning Vendor	Validation requirements and dates are determined by the merchant's acquirer

- The PCI standard requires that companies adhere to a specific set of information security requirements or risk heavy fines and face the possibility of becoming barred from processing credit card transactions:
 - maintain a firewall and intrusion detection system
 - hire an approved third-party auditor to perform quarterly external vulnerability testing
 - monitor file integrity including non-data files
 - render cardholder data unreadable by using one way hash functions, encryption, data truncation, or index tokens
- Companies must maintain an audit trail that dates back at least one year, and implement an incident response plan

Payment Card Industry Data Security Requirements

Build & Maintain a Secure Network
1. Install and maintain a firewall configuration to protect data
2. Do not use vendor supplied default passwords and configuration
Protect Card Holder Data
3. Protect stored data
4. Encrypt transmission of cardholder and sensitive information across public networks
Maintain a Vulnerability Management Program
5. Use & regularly update anti-virus software or programs
6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures
7. Restrict access to 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 a Information Security Policy
12. Maintain a policy that addresses information security for employee and contractors



Confidence in a connected world.

Consequences of non- compliance

Consequence from Banks and Card Companies



- Consequences of non-compliance are imposed by contract:
 - Payment card companies can impose fines
 - Payment card companies terminate the ability to accept payment cards
- Banks are currently paying for the consequences of fraud, and will start imposing fines to recover costs associated with fraud

Reputation Consequences: “TJX data breach: At 45.6M card numbers, it's the biggest ever”



March 29, 2007 ([Computerworld](#)) -- After more than two months of refusing to reveal the size and scope of its data breach, TJX Companies Inc. is finally offering more details about the extent of the compromise.

In filings with the U.S. Securities and Exchange Commission yesterday, the company said 45.6 million credit and debit card numbers were stolen from one of its systems over a period of more than 18 months by an unknown number of intruders. That number eclipses the 40 million records compromised in the mid-2005 breach at CardSystems Solutions and makes the TJX compromise the worst ever involving the loss of personal data.

In addition, personal data provided in connection with the return of merchandise without receipts by about 451,000 individuals in 2003 was also stolen. The company is in the process of contacting individuals affected by the breach, TJX said in its filings.

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9014782&source=NLT_SEC&nid=38

Effects on Other Businesses: “Stolen Data From T.J. Maxx Parent Company Surfaces In Florida Wal-Mart Fraud”



- Data stolen from TJX -- the parent company of T.J. Maxx and other retailers -- has surfaced in the Sunshine State, where it's been used to help thieves steal about \$8 million in merchandise from Wal-Mart stores. The thieves used the stolen TJX customer data to create dummy credit cards for purchasing Wal-Mart and Sam's Club gift cards, and then used those to hit stores in 50 of Florida's 67 counties.

<http://www.informationweek.com/shared/printableArticle.html?articleID=198100636>

Consequences for CIOs: “TJX Intruder Had Retailer's Encryption Key”



TJX is now facing 19 class action lawsuits in the US, and is under a 30-state investigation led by the Massachusetts Attorney General, as well as being investigated by the Federal Trade Commission in the US, and in Canada by the RCMP and both the federal and Alberta privacy commissioners.

'... Not that the culprit necessarily needed it. Data was apparently taken during the card-approval process before it was encrypted. These are among the latest details in what is almost certainly the worst retail data breach ever.

The massive data breach at \$16 billion retailer TJX involved someone apparently armed with the chain's encryption key, but it might not have been needed as the cyber-thief was accessing data during the card-approval process before it was encrypted

...

“It’s incomprehensible that what amounts to a computer worm was placed on mission-critical systems at one of the world’s largest retailers and remained there—undiscovered—for 18 months. The scope of the theft is stunning,” she said. “My biggest fear is that it lays down a gauntlet for other would-be hackers, subtly daring them to ‘top this one.’ It also lays down the gauntlet for other retailers. This could be happening to you right now. PCI compliance and data security do not have obvious return on investment. Neither does paying taxes. But avoiding either can result in irreparable harm.”

<http://www.physorg.com/news94480989.html>



Confidence in a connected world.

How Symantec can help

Symantec Technologies for PCI

Build & Maintain a Secure Network	Product
1. Install and maintain a firewall configuration to protect data	Symantec Security Information Manager Symantec Network Access Control Symantec Endpoint Protection Symantec On Demand Protection
2. Do not use vendor supplied default passwords and configuration	Symantec Control Compliance Suite / Symantec Enterprise Security Manager
Protect Card Holder Data	
3. Protect stored data	Symantec NetBackup Symantec Mail Security Symantec Enterprise Vault Symantec Control Compliance Suite / Symantec Enterprise Security Manager Symantec Vontu Data Loss Prevention
4. Encrypt transmission of cardholder and sensitive information across public networks	Symantec Mail Security
Maintain a Vulnerability Management Program	
5. Use & regularly update anti-virus software or programs	Symantec Endpoint Protection Symantec Mail Security
6. Develop and maintain secure systems and applications	Symantec Control Compliance Suite / Symantec Enterprise Security Manager Symantec Secure Application Services

Symantec Technologies for PCI (2)

Implement Strong Access Control Measures	Product
7. Restrict access to data by business need-to-know	Symantec Control Compliance Suite / Symantec Enterprise Security Manager Symantec Critical System Protection Symantec On Demand Protection Symantec Endpoint Protection Symantec Security Information Manager Symantec Vontu Data Loss Prevention
8. Assign a unique ID to each person with computer access	Symantec Control Compliance Suite / Symantec Enterprise Security Manager
9. Restrict physical access to cardholder data	Symantec Control Compliance Suite
Regularly Monitor and Test Networks	
10. Track and monitor all access to network resources and cardholder data	Symantec Security Information Manager Symantec Control Compliance Suite / Symantec Enterprise Security Manager Symantec Vontu Data Loss Prevention
11. Regularly test security systems and processes	Symantec Control Compliance Suite / Symantec Enterprise Security Manager
Maintain a Information Security Policy	
12. Maintain a policy that addresses information security for employee and contractors	Symantec Control Compliance Suite



Confidence in a connected world.

Conclusion

- Know what is going on: most organizations can't say whether they have been hacked, or are currently being hacked:
 - Symantec Information Security Manager – correlate all the data that you are receiving and understand it
- Assume that someone has gotten in:
 - Vontu DLP – monitor accesses to critical databases containing credit card data and alerting to unusual behaviours
- Enforce and prove your security policies:
 - Symantec Enterprise Security Manager, Symantec Control Compliance Suite – actually enforce the information security policies of your organization and *evidence* it



Confidence in a connected world.

Thank You!

Mark Lewis

Mark_Lewis@symantec.com

416.774.0024

© 2006 Symantec Corporation. All rights reserved.

THIS DOCUMENT IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY AND IS NOT INTENDED AS ADVERTISING. ALL WARRANTIES RELATING TO THE INFORMATION IN THIS DOCUMENT, EITHER EXPRESS OR IMPLIED, ARE DISCLAIMED TO THE MAXIMUM EXTENT ALLOWED BY LAW. THE INFORMATION IN THIS DOCUMENT IS SUBJECT TO CHANGE WITHOUT NOTICE.