Powerful Insights.
Proven Delivery.™

ISACA – Greater Kansas City Chapter

Payment Card Industry (PCI)
Date Security Standards (DSS)

October 8, 2009

Gleb Reznik, PCI-QSA

protiviti®
Risk & Business Consulting.
Internal Audit.

Who We Are

Protiviti **www.protiviti.com** is a global business consulting and internal audit firm composed of experts specializing in risk, advisory and transaction services. The firm helps solve problems in finance and transactions, operations, technology, litigation, governance, risk, and compliance. Protiviti's highly trained, results-oriented professionals provide a unique perspective on a wide range of critical business issues for clients in the Americas, Asia-Pacific, Europe and the Middle East.

Protiviti was formed in May 2002, when Robert Half International (RHI) hired approximately 700 experienced and highly qualified partners and professionals formerly with Arthur Andersen LLP's U.S. internal audit and business risk consulting practices. These practices operated separately from Andersen's external audit and attestation services. Protiviti, which works with over 25 percent of the FORTUNE 500®, employs more than 3,000 professionals in more than 60 locations worldwide. The Company retains the intellectual capital used and developed by its professionals over the past decade.

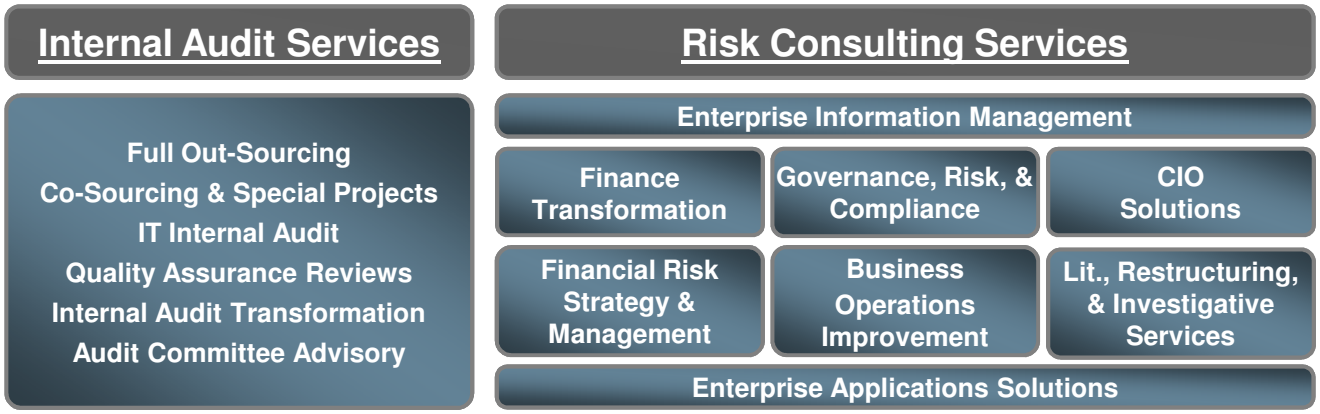
- **Recognized by BusinessWeek for three consecutive years as one of the "Best Places to Launch a Career" (2006-2008)**
- **Named one of "Chicago's 101 Best and Brightest Companies to Work For" by the National Association for Business Resources (2008)**

protiviti®

What We Do

Risk Solutions

Risks can challenge the success of your business from places both inside and outside of your organization. Many of these risks are industry-specific, such as the regulatory concerns within financial services and healthcare. Others are common to all industries, such as supply chain capacity, failed business continuity, financial reporting reliability, lax network security, state of customer relationships and human resources availability. Our integrated risk solutions help you identify, prioritize and manage risks so that you can enhance performance and, ultimately, business value.



Internal Audit

Protiviti provides a full spectrum of services, technologies and skills to management, directors and the internal audit community. We provide world-class people and state-of-the-art methodologies and tools. Our network allows us to offer the right resources, at the right time, in the right place. And we offer a creative and flexible approach to quality assurance reviews, from a standard compliance report to a full transformation of your capabilities. We also provide ongoing assistance for your internal staff and systems.

protiviti®

"It takes twenty years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently."

– Warren Buffett

protiviti®

In the News – T. J. Maxx

T.J. Maxx Hit by Data Breach

Consumer data, including credit card info and driver's licenses, has been stolen from the retailer.

TJ Maxx Data Breach Will Cost Billions

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

It eclipses the compromise in June 2005 at CardSystems Solutions

Reported: January 17, 2007

Number Affected: First Estimation – 45.7 million; Recent Estimation – >100 million

Information Breached: Mix of debit card account numbers, credit card account numbers, and return records containing names and driver's license numbers

How it was Stolen: External source, illegal access to one of the payment systems via insecure wireless transmissions. Hackers collected information for ~17 months before TJX was aware of breach

How Discovered: Self Discovery – identified "suspicious software" on internal systems

Breach Root Cause: Weak network security, lack of data encryption

Governing Judgment: Failure to use "reasonable and appropriate security for sensitive consumer information."

Remediation: Must immediately upgrade and implement comprehensive security procedures, and must submit to audits by third-party security experts every other year for twenty years. TJX offered a three day "customer appreciation" sale at all of it's affiliated stores. TJX also offered free credit monitoring for affected individuals.

OLD NEWS!!

protiviti®

In the News – Heartland

Data breach at Heartland may be bigger than TJX's

Heartland Update: Class Action Suit Filed
Processor Charged with 'Belated and Inaccurate statements' about Breach
January 29, 2009 - Linda McGlasson, Managing Editor

Nation's largest payment processor announces breach in processing system
Posted: Feb 17, 2009 07:12 PM

Reported: January 20, 2009

Number Affected: Specifics unknown; Heartlands processes 100 million credit cards per month

Information Breached: Credit Card Information

How it was Stolen: Malicious software/hack

How Discovered: Third Party - Alerted by Visa and MasterCard of suspicious activity surrounding processed card transactions

Breach Root Cause: Malware attack that compromised card data that crossed Heartland's network

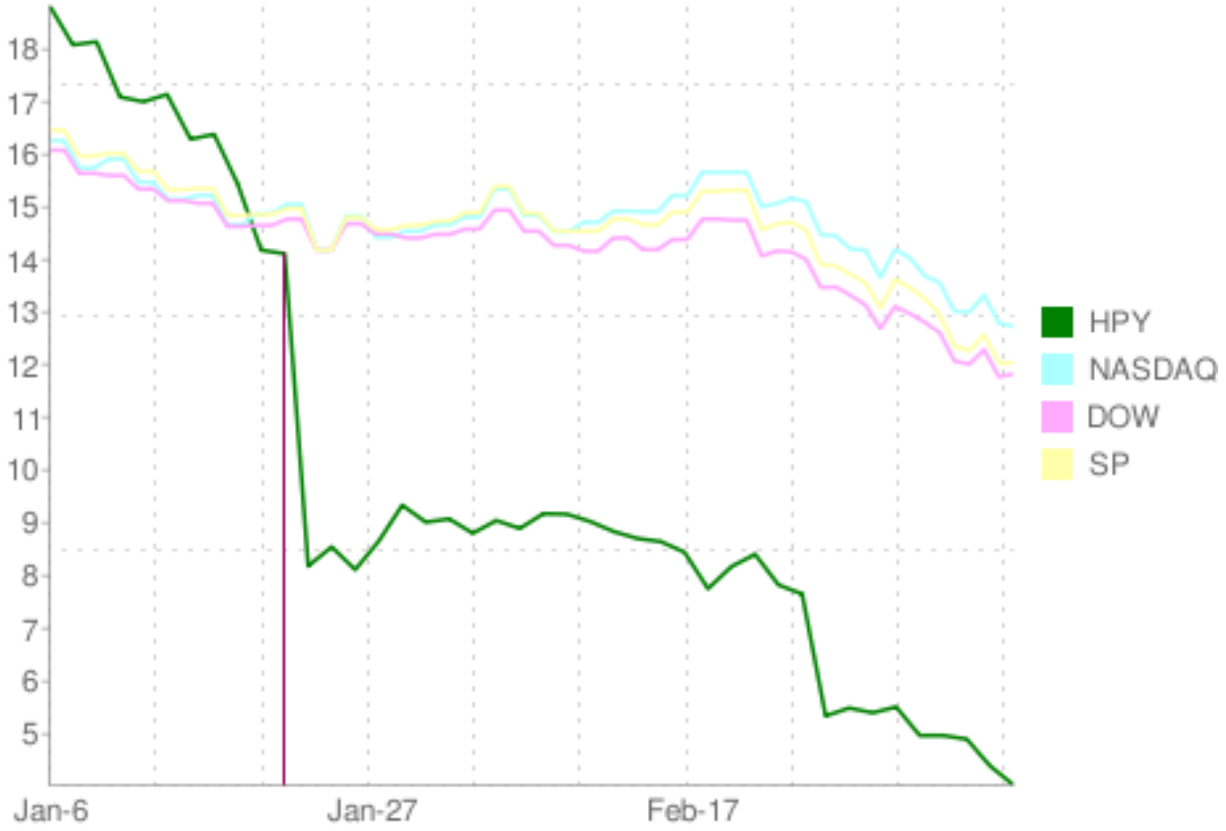
Governing Judgment: Pending litigation alleging Heartland failed to adequately safeguard the compromised consumer data, did not notify consumers about the breach in a timely manner as required by law, and has not offered to compensate consumers for identity theft related costs.

Remediation: Court ruling pending

protiviti®

In the News – Heartland

Heartlands stock price as of the date the incident was reported (1/20/09)



protiviti®

In the News – RBS WorldPay

RBS WorldPay breach exposes 1.5 million
Payment processor buries bad news

Reported: December 23, 2008

Number Affected: 1.5 Million credit card records

Information Breached: Credit Card Information

How it was Stolen: Hack

How Discovered: Self discovery

US arm of RBS faces £141m lawsuit after admitting hackers breached security system

Published Date: 18 February 2009

Breach Root Cause: Malware attack that compromised card data that crossed Heartland's network

Governing Judgment: Pending litigation alleging RBS Worldpay failed to adequately protect the compromised consumer data.

Remediation: Court ruling pending

protiviti®

In the News – Visa

Visa yanks creds for payment card processing pair

RBS, Heartland no longer PCI compliant

- March 13th, 2009 – VISA annouces that RBS WorldPay and Heartland Payments Systems are not on its list of payment card processors who are in good standing with industry-mandated standards for data security.
- RBS expects to recertify its PCI compliance by April of 2009.

protiviti®

In the News – Express Scripts

Extortion Plot Threatens to Divulge Millions of Patients' Prescriptions

By David Kravets | November 06, 2008 | 5:48:54 PM | Categories: Breaches

Reported: November 6, 2008

Number Affected: 75

Information Breached: Names, addresses, birth dates, SSN, Prescription information

How it was Stolen: Unavailable at this time

How Discovered: Third Party – Express Scripts received a ransom letter demanding money from the company under the threat of exposing roughly 50 million records. Seventy-five clients received letters threatening to have information released.

Breach Root Cause: Unavailable at this time

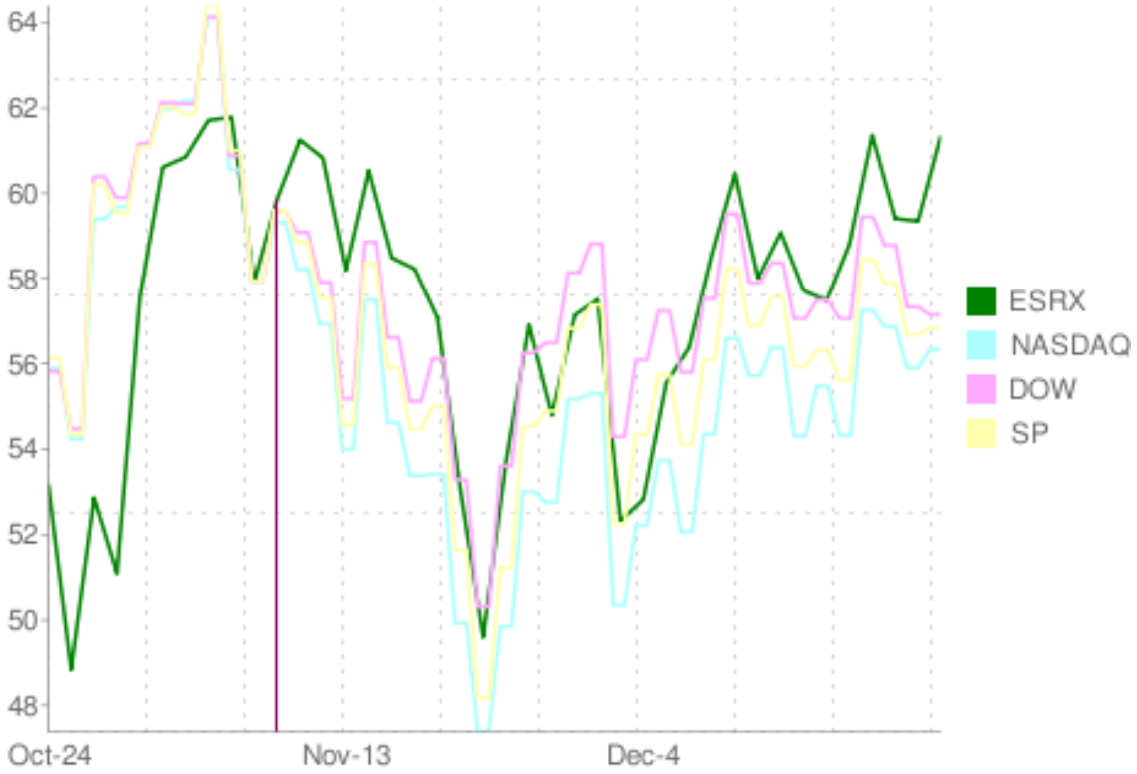
Actions Taken after Identifying Breach: Complying with state notification requirements. FBI Notification immediate after receiving letter.

Remediation: Offering free identity restoration services if becoming a victim

protiviti®

In the News – Express Scripts

Brand and financial Impact



protiviti®

What is PCI?

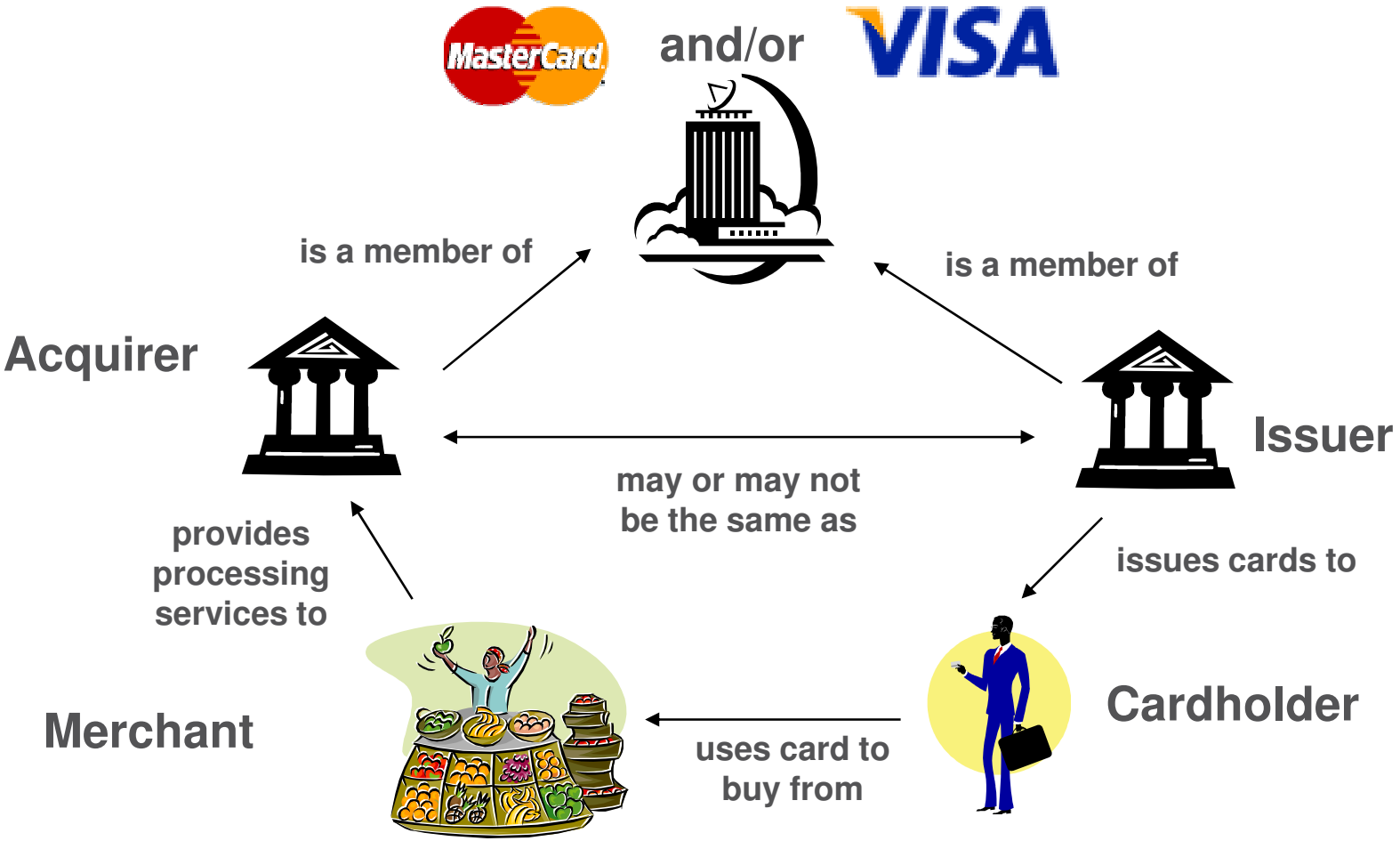
- The PCI (Payment Card Industry) formed to:
  - help prevent credit card fraud
  - reassure consumers
  - Enforce common control practices: the Digital Security Standard, consisting of 6 Principles and 12 requirement

- Administered by PCI Security Standards Council:

www.americanexpress.com www.dinersclubus.com www.discovernetwork.com www.jcbusa.com www.mastercardmerchant.com www.visa.com

protiviti®

PCI Overview



protiviti®

North American Merchant Levels

Level	American Express	MasterCard	Visa USA
1	Merchants processing over 2.5 million American Express Card transactions annually or any merchant that American Express otherwise deems a Level 1	Merchants processing over 6 million MasterCard transactions annually, or compromised merchants	Merchants processing over 6 million Visa transactions annually, identified by another payment card brand as Level 1, or merchants compromised in last year
2	Merchants processing 50,000 to 2.5 million American Express transactions annually or any merchant that American Express otherwise deems a Level 2	Merchants processing over 150,000 MasterCard e-commerce transactions annually	Merchants processing 1 million to 6 million Visa transactions annually
3	Merchants processing less than 50,000 American Express transactions annually	Merchants processing over 20,000 MasterCard e-commerce transactions annually	Merchants processing 20,000 to 1 million Visa e-commerce transactions annually
4	N/A	All other MasterCard merchants	Merchants processing less than 20,000 Visa e-commerce transactions annually, and all other merchants processing up to 1 million Visa transactions annually

protiviti®

MasterCard Validation Requirements

Merchant Level	Onsite Assessment (QSA)	Self Assessment (SAQ)	Network Security Scan (ASV)
1	Required Annually	Not Required	Required Quarterly
2	Required Annually	Required Annually (Until 31 December 2010)	Required Quarterly
3	Not Required	Required Annually	Required Quarterly
4	Not Required	Required Annually	May be required (optional)

** Merchant levels are defined per payment brand. Visa and MasterCard merchant levels are of primary relevance to most organizations as these card types often represent the highest volume of transactions. These merchant level descriptions presented here reflect the revised validation requirements issued by MasterCard on June 15, 2009. Visa merchant levels are similar.*

protiviti®

Service Provider Levels

Level	Description
1	VisaNet processors or any service provider that stores, processes and/or transmits over 300,000 transactions per year.
2	Any service provider that stores, processes and/or transmits less than 300,000 transactions per year.

protiviti®

Implications of MasterCard Validation Requirements

- Level 2 Merchants must have an on-site assessment by 12/31/2010
  - These merchants can no longer use the PCI Self-Assessment Questionnaire (SAQ)
- Level 1 and Level 2 Merchants must engage a PCI-certified Qualified Security Assessor (QSA) to conduct an on-site assessment
  - Internal Audit can no longer perform the assessment
- Many merchants who believe they are compliant may find that they cannot pass an independent assessment conducted by a PCI QSA
  - Higher standards of evidence
  - Scoping
  - Changes in the environment

True or False

As a best practice: **Merchants that have previously self-assessed and need a QSA on-site assessment for 12/31/2010 should engage a QSA Q1 2010 to start the assessment.**

protiviti®

False

- Engage a QSA as soon as possible and conduct the following:
  - Validate scope decisions
  - Walk-through the SAQ
  - Confirm checklist of required activities and associated frequency
  - Discuss evidentiary requirement

- Do this with the QSA on-site, not remotely

protiviti®

PCI Data Security Standard

Objective	Control Area
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 and sensitive information across public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software 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

protiviti®

Non-compliance Is A Problem

Penalties are Severe

- Companies can be **barred from processing** credit card transactions, **higher processing fees** can be applied; and in the event of a serious security breach, **fines of up to $500,000** can be levied for each instance of non-compliance.

Source http://www.internetretailer.com/internet/marketing-conference/80146-compliance-dilemma.html

In case of a compromise, Members proven to be non-compliant or whose merchants or agents are non-compliant may be assessed:

- Non-compliance fine (egregious violations up to $500k)
- Forensic investigation costs
- Issuer/Acquirer losses
  - Unlimited liability for fraudulent transactions
  - Potential additional Issuer compensation (e.g., card replacement)
- Dispute resolution costs
- Disclosure costs

protiviti®

PCI DSS Scoping

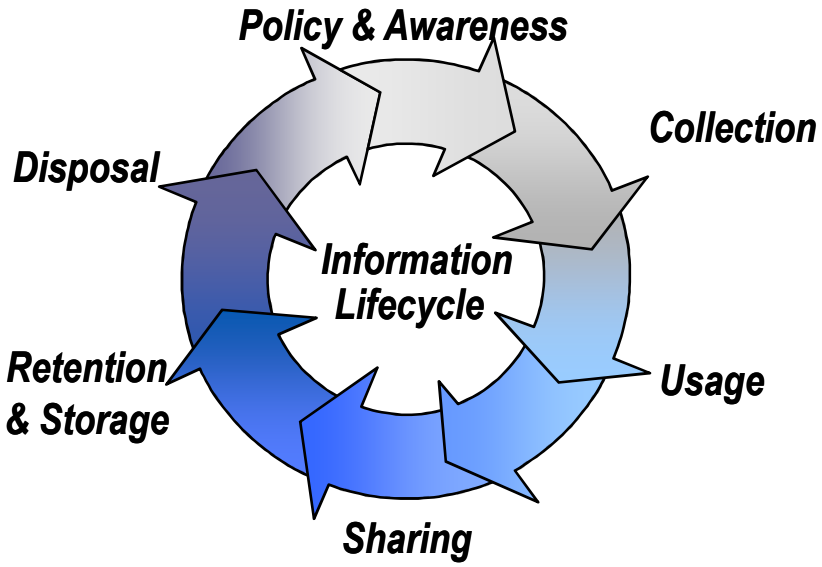
- PCI DSS applies to **all** systems and networks that **store, process, and/or transmit cardholder data**, and **all connected systems**
    - Includes networking equipment that transmits cardholder data (i.e. routers, switches, firewalls, web servers)
    - **Encrypted** cardholder data is **still within scope**
- What is in Scope?
    - Limiting storage of credit card data
    - Segmentation
        - Physical and/or logical
    - PAN truncation
    - PAN hashing (one way hash)
    - Process/Procedure change

protiviti®

Where's the Risk?

Everywhere…

- Management
- Data Privacy
- Information Security
- Physical Security
- Incident Response
- Training and Awareness
- Vendor Management



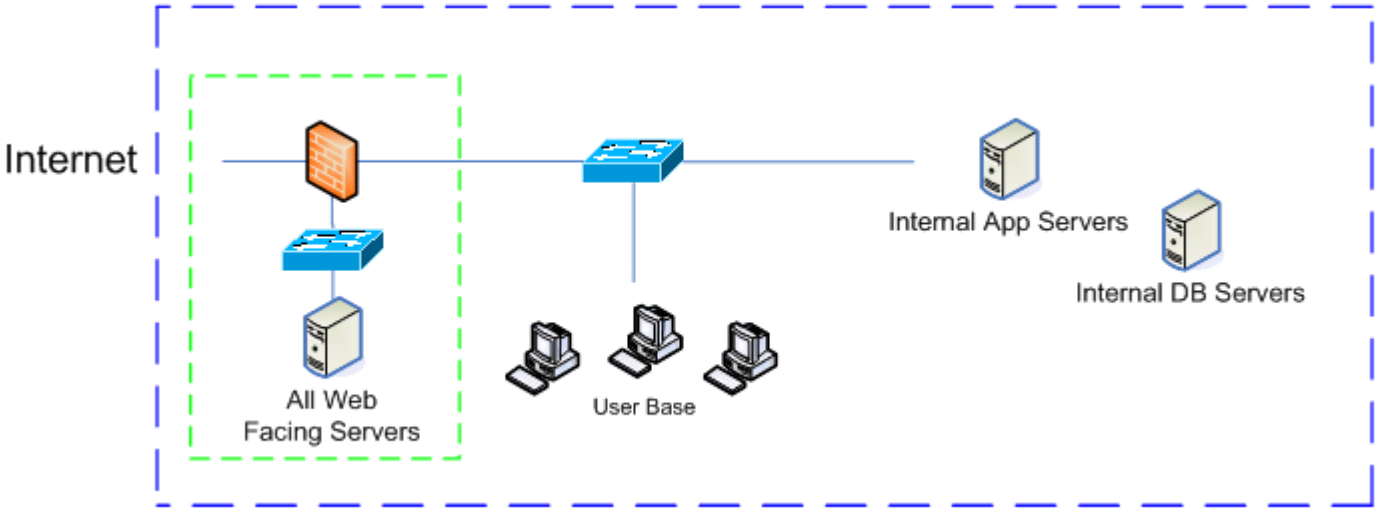
But with a little bit of focus, we can mitigate it…

protiviti®

“We Don’t Store Credit Cards”

- What systems are in scope, if no cardholder data is stored by an organization?
  - Web Servers that maybe obtain credit cards
  - Point of Sale terminals that process transactions
  - Paper repositories

- If you have a “flat network” <u>all systems are in scope</u>



protiviti®

Reducing The PCI Scope

- **Elimination:** Many organizations do not need to store all payment card information – often the data is stored *"because we have always done it that way"*
  - Methods such as PAN truncation and hashing can also achieve this objective
- **Segmentation:** Isolating cardholder systems with network segmentation techniques can reduce in-scope systems
- **Consolidation:** Identifying and eliminating redundant data sets and consolidating applications and information stores can reduce scope
- **Tokenization:** Implementing tokenization methods can reduce encryption requirements and the number of systems in-scope
- **Distributed Processing:** Processing payment cards across multiple Doing-Business-As (DBA) entities can be used to separate compliance reporting
- **Compensating Controls:** Compensating controls that meet the rigor and spirit of the original DSS requirements but at reduced costs can lessen compliance costs / burdens

protiviti®

Compensating Controls

- Assessors can always consider compensating controls (except for track data storage)
- Compensating controls are “above and beyond” other PCI DSS requirements

- Bottom line:
  - Compensating control **must meet** the **intent and rigor of the original PCI requirement** and would withstand a compromise attempt with the same preventive force as the original requirement.

protiviti®

Maintaining PCI Compliance

Three Keys to Success

1. **Know Your Scope**
2. **Strive for Consistency and Standardization**
3. **Manage Change**

protiviti®

Constancy and Standardization

- **Environment Consistency**
  - Implement a common technology infrastructure – POS, network architecture, etc.
- **Process Consistency**
  - Centralized vs. decentralized execution
  - Redundant processes (e.g., change management)
  - Manual processes
  - Higher probability of failure
  - What processes were put in place during with the last assessment?
  - What evidence was “manufactured” during the last assessment?
  - How could manual processes be “semi-automated?” Workflow tool? Service Desk tickets?
- **Document Management**
  - How is substantiating evidence managed?

protiviti®

Managing Change

- **Control "configuration drift"**
  - File Integrity Monitoring & "Closed Loop" Change Management
  - Policy enforcement tools such as Group Policy, Configuresoft, McAfee EPO, etc.
- **Turnover of key personnel**
- **Compensating controls**
  - Do the constraints justifying their use continue to be valid?
- **DSS clarifications, SSC guidance, payment card advisories**

protiviti®

The PCI Compliance Program

- **Maintaining PCI compliance is best achieved by implementing a Compliance Program**
- **Recognize that compliance is not an annual exercise**
  - The Report on Compliance (ROC) or Self-Assessment Questionnaire (SAQ) are used to demonstrate compliance
  - Organizations must continuously comply with all requirements
- **Establish clear responsibility and accountability for compliance**
  - Central person or group should manage compliance across IT and business functions
  - Continuous monitoring of controls and control self-assessment (CSA)
  - Promptly recognize events that may impact compliance and implement / enhance security controls
- **Implement a single program to manage IT security and compliance across various requirements (PCI, SOX, HIPAA, ISO 27001 ISMS accreditation, etc.)**

protiviti®

Contact Information

Gleb Reznik, Manager

protiviti®
Risk & Business Consulting.
Internal Audit.

120 S. LaSalle Ave
Suite 2200
Chicago, IL 60603
Direct: 312.476.6431
Mobile: 773.726.4532

Gleb.Reznik@protiviti.com

Powerful Insights. Proven Delivery.™

protiviti®

Powerful Insights.
Proven Delivery.™

protiviti®