Complying with Payment Card Industry Data Security Standards (PCI DSS) Requirements

Approaches in Higher Education

Dennis W. Reedy

Managing Director, Treasury Operations
Indiana University

September 28, 2010

Agenda

- The bad guys
  - Hostile places, dangerous behavior
  - Data breaches are expensive
- The response
  - Payment Card Industry Data Security Standard
- What it all means for Colleges and Universities
- What Indiana University has done (and learned) as it went through and continues to go though trying to maintain PCI DSS compliance

Security in the News

You Are Vulnerable

SCAM CZARS

What's Russian for 'Hacker'?

By CLIFFORD J. LEVY
Published: October 21, 2007

MOSCOW

PERHAPS the n
the Soviet era w
eye-winking, nir
double-dealing
Ostap Bender. H
antihero of a sat
quest for lost jew
Chairs," but his
law reflected a v

"This misdeed, t
is as innocent as
scheme to use a
identity.

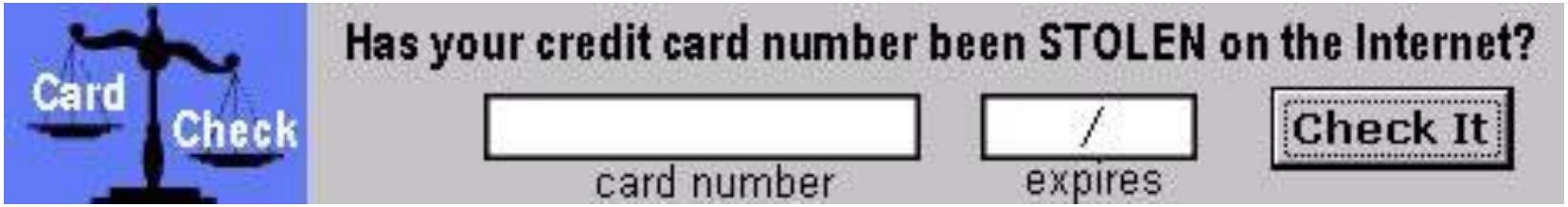
Dan Page

- Plan on it…you will be breached (or you have been, and you don't know it yet)
  - Hackers (sophisticated professionals)
  - Lost/stolen laptop, flash drive
- Thieves target card data
- Active secondary market
  - Dumps, novs, full wallets, dumps with PIN, social engineering, phishing, key loggers, SQL, XSS, sniffers, drive-by, clickjacking …

POS is a Hostile Place

- Older POS terminals and software store track data
- Skimming happens
- August 08: thieves pose as terminal repairmen
- October 08: PIN terminals compromised across Europe

Internet is a Hostile Place



- Some email statistics:
  - 92.3% of email globally was spam
  - 23,300 malicious web pages created every day, or about 1 every 3 seconds
- Your PC online is targeted by hackers every 39 seconds (2,244 times/day)

Commonalities in Breaches

- 66% - victim didn't know they had the data on their systems
- 75% - not discovered by victim
- 83% - attacks not highly difficult
- 85% - opportunistic attacks
- 87% - avoidable through reasonable controls

Breaches are Expensive

- Average cost is $200 per record compromised
- “Small” breach of 5,000 records can cost $1 million
- Brand damage may be greater . Newspapers love to cover the missteps of their local college or university

The Response

- 2001: Visa and MasterCard security standards
- 2004: Standards combined to form DSS
  - Joined by American Express, Discover, JCB
- 2006: PCI Security Standards Council
- 2008: PCI DSS version 1.2, new assessment tools
- 2010: Updated PCI DSS

PCI DSS

Understanding PCI DSS

Control objectives	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 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

5 Stages of PCI Grief

- Denial: It doesn’t apply to me
  - PCI compliance is mandatory
- Anger: It isn't fair
  - PCI applies to everybody
- Bargaining: I’ll do some of it
  - Compliance is “pass / fail”
- Depression: I’ll never get there
  - Many merchants already have
- Acceptance: It’ll be OK
  - PCI addresses things you should already be doing

Some PCI Basics

- If you take plastic, PCI DSS applies to you
  - "Store, process, or transmit" card data
  - POS, e-commerce, moto (mail order/telephone order)… it doesn't matter
  - Size, not-for-profit status don't matter
- Compliance is a contractual obligation
  - Merchant services agreement
- No such thing as "partial compliance"
- Most schools self-assess (SAQ)

Who are the High Risk Merchants?

CISP BULLETIN

Level 4 Merchant Compliance Program Requirements

Risk Consideration	Lower Risk	Higher Risk
Acceptance Channel	Card not present	Card present
Payment Technology	Stand-alone POS terminal	Integrated POS terminal
Transaction Volume	Low	High
Number of Locations	<5	>5
Merchant Category		Restaurants, universities

Understanding PCI DSS

- PCI is a business issue
- Compliance is not optional
- Compliance costs $, non-compliance costs $$$
- Two realities of PCI
  - Your costs will go up
  - You will change the way you do business

PCI Myths

- PCI DSS is an IT project
  - PCI DSS is a business issue
  - PCI DSS is a program, not a project
- They would never fine a university
  - Schools have been fined substantial sums
- PCI is unreasonable and inflexible
  - Nothing alien or new in the standard

PCI Compliance at Indiana University

- Indiana University was certified as compliant on April 1, 2009
- Compliance work began in February 2006
- Treasurer's Office was named the office responsible for achieving compliance
- The Treasurer's Office has always had the responsibility for overseeing the central systems used to process credit cards

IU Enterprise Environment

- 8 Campuses
- 10 Gig connection to the Internet2 backbone
- Multiple commercial internet circuits
- 248 Buildings
- 3,148 Wireless Access Points
- 775 Switches
- 8 Class B subnets
- Multiple Firewalls

IU Merchant Landscape

- Centrally Managed by Treasury Operations
- Over 300 Merchant Locations
- Centralized Systems
  - Dial-up Terminals
  - IPAS-PF (PayPal PayFlow Pro)
- Outsourced Systems
  - NBS QuikPay
  - NBS Commerce Manager
  - Volusion Shopping Cart

IU Merchant Landscape

- Specialty locations with exceptions
  - Hotel
  - Ticketmaster
  - Dining
  - Parking

- 3rd Parties doing business in IU space
  - Barnes & Noble
  - FLIK/Compass
  - Sodexho

PCI DSS Challenges

- Specialty systems managed by departments
  - Several areas involved in PCI compliance initiative
  - Location of servers and systems
- Containing “surprises”. Your PCI DSS project will most likely identify previously unknown business activities
- Cost of firewalls, File Integrity Monitoring, logging solutions
- Multiple solutions vs. Centralized solution

PCI DSS Challenges (continued)

- Indiana University has over 300 unique merchants (university departments) involved in a diverse mix of business activities with multiple locations
- Payments are accepted face to face, via phone and via the internet
- The University uses or contracts with a number of third party providers in connection with processing credit card transactions (e.g. Ticketmaster, Soxedo, Opera, Chartwells, NelNet, US Bank, etc.)

PCI DSS Challenges (continued)

- "We've always done it this way"
- Files (paper and electronic) were full of credit card numbers (especially Bursar, Admissions and Athletics)
- All Indiana University campuses are conveniently "wired" or provide easy access to wireless networks
- Units accepting credit cards do not report to the Treasurer's Office
- Most actions needed to achieve compliance involved "technology" issues (e.g. firewalls)
- No designated funding source to pay for PCI DSS compliance activities

What Indiana University Has Done And Learned From Its Experiences In Becoming And Trying to Maintain PCI DSS Compliance

- Compliance is a Team Effort
- Top Administration must lead and be involved!!!
- Treasury
- Technology
- Purchasing (key player)
- Risk management
- Merchants
- Legal
- Budget Office

- Compliance is Expensive
- Hiring a QSA (Qualified Security Assessor)

  Indiana University uses Trustwave
- Hardware and software
  - Fire walls
  - Separate networks
  - Scans
  - Penetration tests
- Staff time
- Initial and ongoing training!!!!!!!!!
- Approval and exception granting process is challenging!

Key Points

- Start with a Payments Analysis
  - Remember, P-card and travel card data IS credit card data
  - Realistically, you cannot expect to become and maintain compliance until you fully understand the scope of your operations
- Minimize scope
  - If an area or person does not need access to credit card data, do not give it to them
  - If you don't need it, don't keep it
  - Grant as few exceptions as possible
- Review your vendor relationships
  - Are they PA-DSS compliant?

Remember

- Even if your school is compliant: You are only one system change (yours or one of your vendors) away from becoming non-compliant
- The bad guys are out there and they want this data.
- PCI DSS compliance is ongoing and it DOES PERTAIN to each of your institutions.

QUESTIONS?

Acknowledgements & Resources

Special thanks to Walt Conway, QSA, 403 Labs for providing content and examples for this presentation

PCI DSS Council:
www.pcisecuritystandards.org/

Walt Conway, QSA
wconway@403labs.com

Walt Conway's higher education PCI DSS blog:
www.treasuryinstitutepcidss.blogspot.com

Treasury Institute for Higher Education
www.treasuryinstitute.org

Dennis W. Reedy, Indiana University

dreedy@indiana.edu