Recent Developments in PCI DSS

PCI in the Headlines
Risks to Higher Education
PCI DSS Version 1.2
2009 Breach Investigation

- Who did it?
  - 74% external parties
  - 20% insiders
  - 32% implicated business partners
  - 39% involved multiple parties

- How do they happen?
  - 67% victim errors
  - 64% hacking
  - 38% malware
  - 22% privileged user misuse
  - 9% physical attacks
2009 Breach Investigation

- Common elements in breaches
  - 69% discovered by third party
  - 81% of victims were not PCI compliant
  - 83% of attacks not considered highly difficult
  - 87% avoidable through simple or intermediate controls
  - 99.9% compromised records from servers or apps
## 2009 Post-Breach Analysis

<table>
<thead>
<tr>
<th>PCI Requirement</th>
<th>Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Firewall to protect data</td>
<td>30%</td>
</tr>
<tr>
<td>2. Change default or vendor-supplied passwords</td>
<td>49%</td>
</tr>
<tr>
<td>3. Protect stored cardholder data</td>
<td>11%</td>
</tr>
<tr>
<td>4. Encrypt cardholder information across public networks</td>
<td>68%</td>
</tr>
<tr>
<td>5. Update Anti-virus</td>
<td>62%</td>
</tr>
<tr>
<td>6. Develop and maintain secure systems, applications</td>
<td>5%</td>
</tr>
<tr>
<td>7. Restrict cardholder data access to “need to know”</td>
<td>24%</td>
</tr>
<tr>
<td>8. Assign unique IDs</td>
<td>19%</td>
</tr>
<tr>
<td>9. Restrict physical access to cardholder data</td>
<td>43%</td>
</tr>
<tr>
<td>10. Track access to network and cardholder data</td>
<td>5%</td>
</tr>
<tr>
<td>11. Regularly test systems and processes</td>
<td>14%</td>
</tr>
<tr>
<td>12. Maintain security policies</td>
<td>14%</td>
</tr>
</tbody>
</table>
PCI in the Headlines

TJX breach could top 94 million accounts
Filings in case involving Visa cards alone as much as $83 million
By Mark Jewell

BOSTON - At least 94 million Visa and Mastercard accounts could be at risk after an investigation of a credit card fraud

RBS WorldPay breach exposes 1.5 million
Payment processor buries bad news
By John Leyden • Get more from this author
Posted in Security. 29th December 2008 15:03 GMT

USA TODAY

Money » Personal Finance
GET A QUOTE:
Enter symbol(s) or Keywords
GO = DJIA 7,982.54 ▼ -75.27 = NASDAQ 1,636.58

Hackers breach Heartland Payment credit card system
Updated | Comment | Recommend
By Byron Acohido, USA TODAY

Heartland Payment Systems (HPY) on Tuesday disclosed that intruders hacked into the computers it uses to process 100 million payment card transactions per month for 175,000 merchants.
PCI in the Headlines

- Cardholder data breach is not identity theft
- As of today no breached companies have been compliant at time of breach
- In all data breach cases, forensic analysis found significant gaps in PCI controls to be major contributors to the breach
PCI in the Headlines

- Financial damage is bad, Brand damage is worse
- Congressional hearings... national legislation?
Security “Whack-a-Mole”

- PCI increasingly adopted by acquirers
  - Issuers and processors increasingly targeted

- Merchants keep less CHD
  - Thieves seek data-in-transit

- More merchants become PCI compliant
  - More data compromises at smaller merchants

- Better e-commerce security
  - More SQL injection to gain access to payment environment, e.g., through job postings
PCI Lifecycle

1. Market Implementation (10/1/08 – 6/30/09)
2. Feedback Begins (7/1/09 – 10/31/09)
3. Feedback Review and Decision (11/1/09 – 4/30/10)
5. Discuss New Version / Revision (9/30/10)
PCI DSS v1.2

- PCI Version 1.2 effective October 1, 2008
- Update lifecycle: 2 years
- Clarification more than changes
  - Language, terms
  - Eliminate redundancies in previous version
  - Consolidate documentation
PCI DSS v1.2 Changes

- Encryption: user databases
- Wireless: no new WEP after 3/31/09, and none after 6/30/10
- Patches: Install using “risk based” approach
- 6.6 now mandatory
- Secure paper media, too
- Logging: more flexibility
- Pen tests: internal and external, but don’t require QSA/ASV
- Security policies: remote access, wireless, removable media, email, internet usage, laptops, PDAs
- Service providers: policies to monitor and manage them
Scans vs. Penetration Tests

- **Scan (robot; quarterly) vs penetration test (manual; annually)**

- **External pen test**
  - Outward facing IP addresses
  - Hit the firewall, try to get inside

- **Internal pen test**
  - Run from inside, search for vulnerabilities
  - Approach: tester set up as “new user” and tries to get to database server and sensitive data
PCI Council Initiatives

- **PA DSS**
  - Applies to third-party software
  - Includes payment modules of larger systems

- **Quality Assurance Program**
  - Need for consistency: *Hashing with Excel, 20’ Fence, change encryption algorithm annually ...*
  - List assessors “In Remediation”
  - Revocation is an option
  - Rely on Merchant feedback

---

**Appendix C. Sample QSA Feedback Form**

This form is used to review QSAs and their work product, and is intended to be completed after a PCI audit by the QSA client. While the primary audience of this form are QSA audit clients (merchants or service providers), there are several questions at the end, under “QSA Feedback Form for Payment Brands and Others,” to be completed as needed by Payment Brand participants, banks, and other relevant parties. This form can be obtained directly from the QSA during the audit, or can be found online in a useable format at [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org). The client, not the QSA, should submit this form to PCI SSC. Please send this completed form to PCI SSC at: qsa@pcisecuritystandards.org

<table>
<thead>
<tr>
<th>QSA FEEDBACK FORM</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Client Name (merchant or service provider)</strong></td>
</tr>
<tr>
<td>NAME</td>
</tr>
<tr>
<td>CONTACT</td>
</tr>
<tr>
<td>TELEPHONE</td>
</tr>
<tr>
<td>E-MAIL</td>
</tr>
<tr>
<td>Business location where assessment took place</td>
</tr>
</tbody>
</table>
Other PCI Council Efforts

- Unattended Payment Terminals
  - Increasingly used for vending, ticketing
  - Council adopting standards (like PED)

- Special Interest Group (SIG) efforts
  - Two SIGs today (Pre-authorization Data; Wireless)
  - More coming? (Virtualization, Scope, …)
A Prioritized Approach

- Risk-based approach
  - Eliminate account and mag stripe data
  - Secure the perimeter
- A place to start, not a shortcut
- Guidance

The Prioritized Approach to Pursue PCI DSS Compliance

The Payment Card Industry Data Security Standard (PCI DSS) provides a detailed, 12 requirements structure for securing cardholder data that is stored, processed and/or transmitted by merchants and other organizations. By its comprehensive nature, the standard provides a large amount of information about security – so much that some people who are responsible for cardholder data security may wonder where to start the continuous journey of compliance. Toward this end, the PCI Security Standards Council provides the following Prioritized Approach to help stakeholders understand where they can act to reduce risk earlier in the compliance process. No single milestone in the Prioritized Approach will provide comprehensive security or PCI DSS compliance, but following its guidelines will help stakeholders to expedite the process of securing cardholder data.
Visa’s Updated Compliance Framework

- 2009 program to increase compliance and harmonize rules worldwide

- For acquirers
  - Responsible for merchant level validation
  - Use total card volume (*implications for schools?*)
  - Report merchant compliance to Visa twice annually

- For service providers
  - Only Level 1 and Level 2 (no more Level 3)
  - L1 threshold 300,000 transactions/year
  - Only L1 listed on CISP-compliant web page
Some PCI-DSS “Pretty Good” Practices

PCI DSS at Indiana University
Industry Practices
Why “Pretty Good”

WE WILL BE ADOPTING THE BEST PRACTICES IN OUR INDUSTRY, JUST LIKE EVERYONE ELSE.

IF EVERYONE IS DOING IT, BEST PRACTICES IS THE SAME THING AS MEDIocre.

STOP MAKING MEDIOCRITY SOUND BAD!

SORRY.
1. **PCI Gap Analysis**
   - Conduct a Payments Analysis
   - Identify all campus merchants, payment channels (even part-time ones)
   - Identify all vendors and assess compliance
   - Visit each merchant and observe, ask, then ask again
   - Identify gaps and document
   - A simplified SAQ (A - C) may be an objective
2) Remediation

- Prioritize: risk-based approach
- Identify/make the business decisions (often hard!)
- Address the infrastructure changes (expensive)
- Communicate with your acquirer
- Don’t save Policies for the end
- How long does it take...?
Compliance in 3 Steps

3) Validation
   - Prepare the SAQ
   - Document compensating controls (worksheet)
   - Submit SAQ
   - Celebrate... but not for too long...
4) Staying compliant

- You are one system change from being non-compliant
- What makes you think you’re still compliant?
- Are you following all your policies?
  Do you have a new wireless network?
  Did somebody change a firewall rule?
  When did you really last check your logs?

- PCI is a continuing obligation
“Pretty Good” Practices at Indiana University

- Top management commitment
  - Board of Trustees and Treasurer
- Centralize payment card operation
  - Office of Treasurer manages acquirer and policies
- Incidence Response Plan
  - itso.iu.edu/Incident_Response
- Communicate
  - Quarterly newsletter
Training at Indiana University

- Revenue Processing training on each IU campus
  - Offered once per year on each campus, twice at Bloomington and Indianapolis
  - Training required for all full time staff processing revenue
  - Always available - go to any campus
  - Office of Treasurer can provide individual training where warranted (e.g., major turnover)

- Over 1,200 individuals trained
Other Office of Treasurer support:
- Web-based tutorial
- PCI DSS link on website: indiana.edu/~iutreas
- Full day e-Business and Banking Seminar each summer (Indianapolis and Bloomington)
- Quarterly newsletter to 1,100+ people

Technical PCI training through UITS
Other “Pretty Good” Practices

- Find and eliminate track data
  - Reduce potential liability 90%
  - Vendors may not be much help
  - Sensitive number finder can locate rogue databases

- Upgrade POS terminals to truncate PANs on both copies

- Find rogue payment sites on your campus(es)
  - Google news alert
Other “Pretty Good” Practices

- Think before you act, or “PCI Requirement 0”
  - Understand “cardholder data” and “cardholder data environment”
  - Understand PCI before implementing solutions

- Eliminate storing cardholder data...
  Then tell people about it!
Other “Pretty Good” Practices

- Monitor card alerts and bulletins
  - Visa Data Security Alert
    - SQL Injection Attacks
    - January 25, 2008
    - To promote the security and integrity of the payment system, Visa is committed to helping financial institutions and payment system participants better understand their responsibilities.
    - Recommended Mitigation Strategy
      - To minimize the possibility of a SQL injection attack and mitigate the risk of a data compromise.

- Monitor PCI and security blogs and forums
  - Keep up to date
  - Ask questions, get expert help
  - Collaborate: share experiences, good and bad

- Use the PCI SSC resources
  - Audit Guidelines
  - Technical FAQ
Other “Pretty Good” Practices

- Raise security awareness on campus
- Identify repeat offenders who lose (stolen) devices, download malware, etc.
  - Publicize names
  - Consequences

---

**The Wired Campus**

Education-technology news from around the Web

**November 13, 2008**

*Tech-Security Official at U. of Virginia Wears Fish Costume to Raise Awareness of 'Phishing'*

When Karen McDowell dressed up in a purple fish costume and walked around the University of Virginia’s campus last month, she got plenty of attention for her cause, even though she had to explain the meaning of her outfit. Ms. McDowell is a security analyst for the university, and her goal was to raise awareness about e-mail phishing schemes, in which con artists send e-mail messages hoping to lure people into giving out their passwords or other personal information.

“Sometimes I introduced myself as a fraudulent e-mail because many people don’t know what a phish is,” said Ms. McDowell (pictured in costume, at right).

In fact, pulling off her plan of dressing up as a “phish” for Cybersecurity Awareness Month was more difficult than she had expected. She could not find a fish costume online.
Other “Pretty Good” Practices

- Develop and promote payment policies
- **Re-train** POS staff
- Develop a user manual
  - New merchants
  - Guidelines
  - Responsibilities
  - Costs
  - Merchant agreement
Other “Pretty Good” Practices

- Use PCI Council’s PA DSS list for third-party applications
  - On Council’s website

- Use Visa’s CISP list for third-party service providers
  - New service provider levels in 2009
  - Only Level 1 will be listed on Visa website
PCI and Beyond

- PCI does not make you secure
- Map your payment data flow
- Monitor service providers and vendors
  - Use strong passwords for technical support
  - Log tech support and third-party access
- Upgrade POS equipment and payment apps
- Beware of rogue wireless networks
- Perform vulnerability scans monthly
- Go beyond: apply PCI to all your PII
Thank You

☐ Your Thoughts, Comments, Questions

walt@walterconway.com

www.walterconway.com