PCI DSS in Context

Some History
Key Players
Validating Compliance
Cardholder Data
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
First, Some PCI Basics

- PCI DSS: Payment Card Industry Data Security Standard

- Goal is to protect “Cardholder Data” (CHD)
  - Primary Account Number (PAN)
  - Also addresses track data, security codes, PINs

- If you take plastic, PCI applies to you
  - “Store, process, or transmit” cardholder data
  - P-cards, travel cards may be in scope

- PCI Compliance is by institution

- Most schools use Self-Assessment Questionnaire (SAQ)
# PCI DSS: 6 Goals, 12 Requirements

<table>
<thead>
<tr>
<th>Control Objectives</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Build and maintain a secure network</td>
<td>1. Install and maintain a firewall configuration to protect cardholder data</td>
</tr>
<tr>
<td></td>
<td>2. Do not use vendor-supplied defaults for system passwords and other security parameters</td>
</tr>
<tr>
<td>Protect cardholder data</td>
<td>3. Protect stored cardholder data</td>
</tr>
<tr>
<td></td>
<td>4. Encrypt transmission of cardholder data across open, public networks</td>
</tr>
<tr>
<td>Maintain a vulnerability management program</td>
<td>5. Use and regularly update anti-virus software</td>
</tr>
<tr>
<td></td>
<td>6. Develop and maintain secure systems and applications</td>
</tr>
<tr>
<td>Implement strong access control measures</td>
<td>7. Restrict access to cardholder data by business need-to-know</td>
</tr>
<tr>
<td></td>
<td>8. Assign a unique ID to each person with computer access</td>
</tr>
<tr>
<td></td>
<td>9. Restrict physical access to cardholder data</td>
</tr>
<tr>
<td>Regularly monitor and test networks</td>
<td>10. Track and monitor all access to network resources and cardholder data</td>
</tr>
<tr>
<td></td>
<td>11. Regularly test security systems and processes</td>
</tr>
<tr>
<td>Maintain an information security policy</td>
<td>12. Maintain a policy that addresses information security</td>
</tr>
</tbody>
</table>
The “cardholder data environment” can include:
- Network components (firewall, switches, routers...)
- Servers (web, database, mail...)
- Applications (purchased, custom, internal, external)
- Policies, procedures

 Anything that stores, transmits, or processes cardholder data is in scope

 “If you don’t need it, don’t keep it”
Global forum to enhance global payment security
  - PCI DSS, PA DSS, PIN PED

Approve assessors (QSAs) and scan vendors (ASVs)

Develop Self-Assessment Questionnaires (SAQ)

Develop and publish PCI documentation
Key Players

- Participating Organizations provide a voice for merchants and processors

- Participating Organizations include NACUBO with Treasury Institute for Higher Education
  - A voice for Higher Education
  - Tom Davis of IU is technical representative
Key Players

- Five Payment brands
  - Track compliance and enforce standards (fines, sanctions)
  - Determine event response (forensics)
  - Define merchant levels

- Acquirers (Merchant Banks)
  - Set merchant level
  - Certify compliance
  - Approve compensating controls
The PCI Chain

- Payment Brands
- Acquirer
- Payment Processor
- Merchant
- 3rd Party Service Provider
Cardholder Data

- **PAN**
  - **Credit Card**
  - **Expiration date**

- **CID**
  - (American Express)

- **CAV2/CID/CVC2/CVV2**
  - (all other payment brands)

- **Magnetic stripe**
  - (data on tracks 1 & 2)
Quiz:
Which are “Cardholder Data?”

- Name + expiry date + service code
- 1234 5678 9012 3456 + name + expiry date
- 1234 56xx xxxx 3456 + name + expiry date
- 1234 56xx xxxx 3456 + name + CVV2
- 1234 5xxx xxxx2 3456 + name
- Name + expiry date + service code + signature
Why Are You Keeping Those Data?

- Policy: Store no PANs on campus...anywhere

- But what about ...?
  - Recurring payments - acquirer has alternatives
  - Chargebacks, refunds - let acquirer store PAN data
  - Legal requirements - these apply to banks, not you
  - Paper receipts - upgrade terminals to truncate PAN on both copies
  - POS software stores PANs - reconfigure or replace
  - P-cards and travel cards - yes, they are in scope
Validating Compliance

- Validation is by institution

- Don’t confuse Merchant Level and Merchant ID
  - Level is for compliance validation
  - ID is for accounting
  - Acquirer may combine IDs for PCI validation

- Simplified SAQs
  - Four versions: depends on card environment
  - Limiting PCI scope simplifies validation
  - Common element: no electronic cardholder data
Visa Inc. Cardholder Information Security Program (CISP)  
U.S. PCI DSS Compliance Validation Update as of 12/31/08

<table>
<thead>
<tr>
<th>CISP Validation Category (Visa transactions / year)</th>
<th>Population</th>
<th>Estimated % of Visa Transactions</th>
<th>PCI DSS Compliance Validated***</th>
<th>Initial Validation Submitted / Remediating</th>
<th>Initial Validation In Progress</th>
<th>Pending Commitment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1 Merchants (&gt; 6M)</td>
<td>362</td>
<td>50%</td>
<td>91%</td>
<td>9%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>Level 2 Merchants (1 – 6M)</td>
<td>702</td>
<td>13%</td>
<td>87%</td>
<td>11%</td>
<td>2%</td>
<td>0%</td>
</tr>
<tr>
<td>Level 3 Merchants (e-commerce only 20,000 – 1M)</td>
<td>2627</td>
<td>&lt; 5%</td>
<td>57%</td>
<td>19%</td>
<td>23%</td>
<td>1%</td>
</tr>
</tbody>
</table>

1 - Validation statistics are based on merchant compliance reporting provided by acquirers.
2 – Excludes 272 Level 2 merchants identified in 2007 which were required to validate compliance by 12/31/08.

Noteworthy, 99% of Level 1 and 2 merchants confirmed that they do not store prohibited data. Acquirers of Level 1 and 2 merchants that continue to store prohibited data are subject to monthly fines.
Security

The Bad Guys

Higher Ed top 10 Threats

The Insider Threat
Five emerging threats

- Malware
- Botnets
- Cyber warfare
- VoIP and mobile devices
- Evolving cyber crime economy

“Data will continue to be the primary motive behind future cyber crime.”
PCI DSS’ Role

- The purpose of PCI DSS:
  - To protect cardholder data
  - To keep you and your institution out of the headlines

- PCI is a data protection standard
  - Not a fraud prevention measure
  - PCI does not make you secure
Gone Phishing

From: United States District Court [subpoena@uscourts.com]
To: Steve Kirsch
Cc: 
Subject: Subpoena in case #28-755-YCH

AO 88(Rev.11/94) Subpoena in a Civil Case

Issued by the
UNITED STATES DISTRICT COURT

Issued to: Steve Kirsch
Propel Software Corporation
408-571-6300

SUBPOENA IN A CIVIL CASE

Case number: 28-755-YCH
United States District Court

YOU ARE HEREBY COMMANDED to appear and testify before the Grand Jury of the United States District Court at the place, date, and time specified below.

Place: United States Courthouse
880 Front Street
San Diego, California 92101

Date and Time: May 7, 2008
9:00 a.m. PST

Room: Grand Jury Room
Some Links are Good, Others

Microsoft: Rogue AV Found On 10 Million Machines

Scareware more pervasive than thought, while data breaches more about lost and stolen equipment than hackers, according to new Microsoft Security Intelligence Report

Apr 08, 2009 | 11:06 AM

By Kelly Jackson Higgins

DarkReading

Rogue security software infections by just one family of malware jumped 66 percent in the second half of the year, according to Microsoft’s new Security Intelligence Report (SIR), released today. And it’s not hackers who are responsible for data breaches: it’s the lost and stolen laptops, disks, and other computer equipment, according to the report.
Are Users Listening? Is Anybody Listening?

Source: Psychology Department, North Carolina State University
Higher Ed “Top 10 Security Threats

1. Malware, botnets
2. Thieves
3. Staff members
4. Professors
5. Students
6. Outsource partners
7. Social networks
8. Phishing
9. Cell Phones
10. Spammers
The Insider Threat

- **Well-intentioned staff**
  - Just trying to do their jobs

- **Self-interested or malicious staff**
  - Intentionally download apps or visit prohibited sites
  - Economy is affecting this group

- **Trusted partners**
  - Third-parties with insider privileges

![Comic strip](https://www.dilbert.com/)
The Insider Threat

- 20% of users changed security settings to access unauthorized websites
- Over 80% of enterprises show Google application activity, and nearly all evidence peer-to-peer applications
- 35% of users consciously violate internal security policies (to expedite their work)
- Over 50% of employees who left their job in 2008 took some company confidential information with them
People under the age of 28 are engaging in online behavior that could expose their organizations to data leakage and theft.

60% of young staff "are either unaware of their companies' IT policies or are not inclined to follow them."

IT Security's Next Big Threat: Young People

Generation Y user behavior could endanger security of enterprise systems, studies say

By Tim Wilson, DarkReading
Nov. 19, 2008
Security: Why Care?

- Expense: lawsuits, financial liability, fixing systems
- Lost productivity
- Reputation (brand)
- State laws requiring notification...and often more
- The number of Higher Ed breaches is too high
Security: Why Care?

The Wired Campus
Education-technology news from around the Web

April 9, 2008
At Least 86 Campuses Have Been Hit in E-Mail 'Phishing' Scam

An informal survey conducted this week on an e-mail list for campus IT administrators indicated that at least 86 colleges and universities have been hit by e-mail 'phishing' scams.

As more colleges have been hit by these scams, some administrators are calling for heightened awareness and education about the risks of these scams.

Con Artists Attack Colleges With Fake Help-Desk E-Mail

By JEFFREY R. YOUNG

An e-mail scam has hit tens of thousands of users at dozens of colleges over the past few weeks, leaving network administrators scrambling to respond before campus computer accounts are taken over by spammers.

Students, professors, and staff members at the affected colleges received e-mail messages that purported to come from the colleges' help desks, asking users to reply with their log-in and password, and in some cases other personal information including birth date.

Conflcker Infects More Than 700 Computers at U. of Utah

The latest variant of the Conflcker worm—sophisticated computer malware that uses the Internet to invade and extract data from computers running Windows operating systems—infected between 700 and 800 computers at the University of Utah, primarily ones belonging to faculty and staff members in the university’s health-sciences center.

Officials at the university are saying that computer systems on campus were not affected.
Breaches are Expensive

- Benchmark: $197 per account compromised
- “Small” breach (5,000 accounts) can cost $1 million
- Brand risk is bigger
- PCI compliance is not just required, it makes good business sense
PCI Conclusions

Getting PCI Compliant

Staying Compliant

Do the Math

The Reality of PCI
You’re compliant… so order some pizza but don’t relax too much

PCI is backward looking
  - Compliance today says nothing about tomorrow

You are one system or process change from being non-compliant
  - Establish and follow policies
  - Educate, train, communicate
“But we outsourced our e-commerce”
- Staff use PCs to enter MOTO transactions

“P-cards and travel cards don’t count”
- If you store the PANs, they can be in scope

“We didn’t know we stored the data”
- Non-compliant POS devices, PCs, servers, ...
Do the Math...

- \( V \neq C \)
  - System change, not following policies, ...

- \( C \neq S \)
  - PCI is a data protection standard

- So what makes you think \( V = S \)?

- For advanced pupils: \( S \leq 100\% \)
  - There is no such thing as perfect security
The Reality of PCI

- Compliance is a journey, not a destination
- Compliance takes resources
  - People
  - Business practices
  - Technology
  - Budget
- PCI is not going away
The Reality of PCI

- Your costs will go up
  - Cost to get and remain PCI compliant
  - Non-compliance costs more

- You will change the way you do business
  - Do you want to be in the payment business?
  - Maybe fewer campus merchants take plastic
  - Limiting access to cardholder data

- Conclusion: PCI is a business issue
Conclusions

- Take control – You can’t outsource responsibility
- PCI training has a very high ROI!
- Senior management commitment and multidisciplinary team are critical
- Network with other institutions
- If you don’t need it, don’t keep it
Higher Education
Community Resources

- The Treasury Institute for Higher Education: www.treasuryinstitute.org
- PCI blog: www.treasuryinstitute.org/blog
- NACUBO: www.nacubo.org
Additional PCI Resources

- Society of Payment Security Professionals: www.paymentsecuritypros.com
  - Blogs, PCI forum

- PCI SSC: pcisecuritystandards.org
  - Standards, FAQ, PA DSS

- Visa: visa.com/cisp
  - PCI-compliant service providers

- MasterCard: mastercard.com/us/sd
5 Stages of PCI Grief
Have You Moved Up a Stage?

- **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
Understanding and Managing PCI DSS

- YOUR thoughts? Comments? Questions?

walt@walterconway.com

www.walterconway.com