PCI DSS 3.0 Changes & Challenges

EVAN FRANCEN, CISSP CISM
PRESIDENT/CO-FOUNDER FRSECURE
PCI DSS 3.0 Changes & Challenges

Topics

• FRSecure, the company
• Introduction to PCI-DSS
• Recent breaches
• Recent PCI-DSS changes
• State of the industry
• Pragmatic approach to compliance
• Common mistakes
• Questions
PCI DSS 3.0 Changes & Challenges

Our Agenda

• FRSecure, the company
• Introduction to PCI-DSS
• Recent breaches
• Recent PCI-DSS changes
• State of the industry
• Pragmatic approach to compliance
• Common mistakes
• Questions
FRSecure, the company

We exist “to fix a broken industry”

We are an information security consulting and management company; it’s all that we do.

FRSecure’s Security Ten Commandments

1. A business is in business to make money
2. Information Security is a business issue
3. Information Security is fun
4. People are the biggest risk
5. “Compliant” and “secure” are different
FRSecure, the company

We exist “to fix a broken industry”

We are an information security consulting and management company; it’s all that we do.

**FRSecure’s Security Ten Commandments**

6. There is no common sense in Information Security

7. “Secure” is relative

8. Information Security should drive business

9. Information Security is not one size fits all

10. There is no “easy button”
FRSecure, the company

We exist “to fix a broken industry”

Our Services:
• PCI Compliance; we are a QSA
• Information Security Assessments
• Regulatory Compliance; HIPAA, GLBA, etc.
• Security Program Development
• SOC 2 Readiness
• Training & Awareness
• Social Engineering
• Penetration Testing
Introduction to PCI-DSS

History

• Between 1988 – 1998 Visa and MasterCard report $750 million in credit card fraud losses
• **October 1999**, Visa approves the Cardholder Information Security Program (CISP) – the 1st precursor to PCI-DSS
• **December 2004, PCI-DSS v1.0** debuts – the 1st unified (among all five major card brands) security standard and compliance is mandatory (for 20,000 or more transactions)
• **September 2006, PCI-DSS v1.1** – requires independent code reviews and/or Web application firewalls (requirement 6.6), the PCI SSC is born.
• **December 2006, TJX data breach** – insecure wireless network and 45 million TJX customers affected.
• **October 2008, PCI-DSS v1.2** – new requirements for wireless networks and AV for all systems.
• **January 2009, Heartland breach** (breach actually occurred in 2008) – 130 million payment records
• **October 2010, PCI-DSS v2.0** – no major surprises
• August 2012, Visa claims that 97% of Level 1 merchants are “compliant”
• **November 2013, PCI-DSS v3.0** – We’ll cover changes in v3.0 and since...
Introduction to PCI-DSS

PCI-DSS v3.0

• Latest version, released in November, 2013
• Key themes emphasized throughout Version 3.0 include:
  • Education and awareness
  • Increased flexibility
  • Security as a shared responsibility
• Change types include “Clarification”, “Additional guidance”, and “Evolving Requirement”
• Final PCI-DSS v3.0 can be found here;
Introduction to PCI-DSS

PCI-DSS v3.0

• Latest version, released in November, 2013

• Change highlights -

• Key themes emphasized throughout Version 3.0 include:
  • Education and awareness
  • Increased flexibility
  • Security as a shared responsibility

• Change types include “Clarification”, “Additional guidance”, and “Evolving Requirement”

• Final PCI-DSS v3.0 can be found here;
Recent breaches

Target

- Est. 45 million credit & debit cards
- Contributing factors:
  - Vendor access
  - Single-factor/weak authentication
  - Memory-scraping malware on registers
- Target was issued a PCI Report on Compliance (ROC) by Trustwave
- The breach went undetected for more than two weeks
- Gathered tons of public attention and led to numerous lawsuits
- CEO and CIO gone
Recent breaches

Home Depot

- September, 2014
- Est. 56 million credit & debit cards
- Contributing factors:
  - Vendor access
  - Single-factor/weak authentication
  - Memory-scraping malware on registers
- Home Depot was issued a PCI Report on Compliance (ROC) by ???
- The breach went undetected until notification by 3rd parties.
- As many as 44 civil lawsuits, government investigations, and millions in losses.
- Ricky Joe Mitchell – convicted in May, 2014 of sabotaging his former employer’s network.
- “Who cares, we sell hammers”, CEO (Frank Blake) had already announced retirement (on August 21st)
Recent PCI-DSS Changes

PCI-DSS v3.0 (and revisions)

• Overview; there are twelve (12) requirements:
  • BUILD AND MAINTAIN A SECURE NETWORK
    • Requirement 1: Install and maintain a firewall configuration to protect cardholder data
    • Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
  • PROTECT CARDHOLDER DATA
    • Requirement 3: Protect stored cardholder data
    • Requirement 4: Encrypt transmission of cardholder data across open, public networks
  • MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM
    • Requirement 5: Use and regularly update anti-virus software
    • Requirement 6: Develop and maintain secure systems and applications
  • IMPLEMENT STRONG ACCESS CONTROL MEASURES
    • Requirement 7: Restrict access to cardholder data by business need-to-know
    • Requirement 8: Assign a unique ID to each person with computer access
    • Requirement 9: Restrict physical access to cardholder data
  • REGULARLY MONITOR AND TEST NETWORKS
    • Requirement 10: Track and monitor all access to network resources and cardholder data
    • Requirement 11: Regularly test security systems and processes
  • MAINTAIN AN INFORMATION SECURITY POLICY
    • Requirement 12: Maintain a policy that addresses information security
Recent PCI-DSS Changes

PCI-DSS v3.0 (and revisions)

First major change:

PCI – Payment Card Industry name change to

PCI – Pay Cash Instead

You were supposed to laugh.
If you did not laugh, please do so now.
Recent PCI-DSS Changes

PCI-DSS v3.0 (and revisions) – Seriously...

• Expect audits to be more thorough and less acceptance of mitigating controls
  • The goals of PCI, retailers and QSA don't often align
• PCI-DSS should be viewed as a “base level” of security only
• PCI-DSS should be part of “Business-as-Usual Processes”
• Use past breaches as a method to predict what will be coming further down the road.

• More emphasis placed on:
  • Education and awareness
  • Security as a shared responsibility
  • Network segmentation/isolation

“I work at a tier 1 PCI merchant and I can tell you that it is a sham. We use an external auditor but it doesn't make any difference. These audits are too simple and the people performing them are completely outmatched by their adversaries.”
Recent PCI-DSS Changes

PCI-DSS v3.0 (and revisions) – Seriously...

• For all the details of the changes from v2 to v3.0, see https://www.pcisecuritystandards.org/documents/PCI_DSS_v3_Summary_of_Changes.pdf. There are too many for a one hour presentation.

• Also see the standard itself, here: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

• The scope of what applies to PCI compliance was greatly clarified.

• How audits should be conducted was greatly clarified.

• If you are responsible for PCI compliance, you should definitely read the documents listed above.
Recent PCI-DSS Changes

PCI-DSS v3.0 (and revisions) – Seriously...

Bulletins are routinely issued by the PCI-SSC; the latest is an impending revision to PCI-DSS dated 13 February 2015

“no version of SSL meets PCI SSC’s definition of “strong cryptography,” and revisions to the PCI Data Security Standard (PCI DSS) and the Payment Application Data Security Standard (PA-DSS) are necessary”

SSL will no longer be compliant – migrate all systems and work with vendors to replace SSL with TLS
State of the industry

There is plenty of confusion.

• Many Level 1 Merchants are having issues under the additional scrutiny from QSAs
• Additional scrutiny is being placed on smaller merchants
• Smaller merchants aren’t really sure how to comply; which requirements apply and how to demonstrate compliance
• Not only are merchants confused, but so are many security consultants

Ever had a PCI audit or consultant show you where you’re not compliant, but not show you how you can comply?
Pragmatic approach to compliance

There best answer to confusion is to *simplify*
Pragmatic approach to compliance

1. **PCI-DSS Scoping**
   - PCI-DSS compliance **only** applies to the **Cardholder Data Environment (or “CDE”)**
   - So what is the Cardholder Data Environment?
   - **Reduce scope** whenever possible!

*The cardholder data environment (CDE) is comprised of people, processes and technologies that store, process, or transmit cardholder data or sensitive authentication data. “System components” include network devices, servers, computing devices, and applications.*

**In other words...**

Any system that affects the security of cardholder data (including authentication data) is in-scope; including systems that can affect the security of a system that affects the security of cardholder data.
Pragmatic approach to compliance

2. PCI-DSS Gap Analysis

- Now that you know what PCI-DSS compliance applies to, figure out what requirements apply
- Which requirements apply, depends on how you are using cardholder data

Process less than 6,000,000 card transactions annually?*

I can do a Self-Assessment Questionnaire (or SAQ), but which one?

There are four major types; A through D. The type of SAQ will determine which requirements apply to your CDE.
Pragmatic approach to compliance

3. PCI-DSS Consulting

- Undergo efforts to reduce scope (CDE).
- Undergo efforts to reduce the number of requirements that apply.
- Undergo efforts to apply the necessary controls to comply with the remaining PCI-DSS requirements.

Keep in mind that the controls will need to be sustainable and become “Business-as-Usual”.
Pragmatic approach to compliance

4. **PCI-DSS Audit**
   - Conduct your own audits, regardless of whether or not you engage a QSA.
   - Audits can get very detailed and some requirements may be open to interpretation. If using a QSA, the QSA has the final say.
   - Maintain evidence and pay special attention to “mitigating controls”

Keep in mind that the controls will need to be sustainable and become “Business-as-Usual”.
Pragmatic approach to compliance

5. Business-as-Usual

- Operate the business according to the PCI-DSS requirements
- Consider the requirements whenever changing business processes or adding services.
- There are quarterly requirements (scanning)
- Annually, you should restart the entire process. Do not assume anything.
Common mistakes

1. Management does not get involved enough
2. Merchants and QSAs have an unhealthy relationship
3. The scope of the CDE is not correct
4. The commitment made by the merchant is only to comply, not to incorporate as “Business-as-Usual”
5. Cutting corners (the letter vs. the intent)
Questions

Questions?

What things would you like to see next time or have to help you in your efforts?

Thank you!

Are there any questions that can’t be answered with Google?