PCI Program Frameworks – Learning to Cope with Compliance

Daniel Adinolfi – Cornell University
David Escalante – Boston College
We will cover...

- General PCI mindsets.
- The ins and outs of Scoping, including some tricky edge cases.
- Governance Frameworks to help manage the PCI burden.
You will...

- Review some PCI basics.
- Debate and discuss some scoping examples.
- Work with your peers to explore the process of creating frameworks.
- Understand why PCI is a bit like Dr. Strangelove’s subtitle
Introductions (Us)

- David Escalante, Director of Computer Security, Boston College.
  - BC is a Level 3 merchant.
  - Around 50 MIDs
  - Centralized IT governance.
  - Centralized Finance governance.

- Daniel Adinolfi, Senior Security Engineer, Cornell University
  - Cornell is a Level 3 merchant.
  - Over 300 MIDs.
  - Distributed IT governance.
  - Hybrid Finance governance.
Introductions (You)

- Tell us about you!
  - What Level Merchant are you?
  - Who is from a private/public institution?
  - Who is new to PCI?
PCI Mindsets

- PCI should be a risk reduction exercise
  - Risks include reputation loss, monetary loss, compliance failure.
  - Nothing to do with security, but N.B.
    - Many PCI requirements are best practices.
    - Post-PCI you may be more secure
  - Should be part of your larger compliance program.
Scoping Scenarios

Questions to consider for each scenario:
- What ends up in scope and why? For example:
  - What networks are in play?
  - What cards and processors are in play?
  - What kind of devices are taking cards?
- Is it possible to reduce scope?
- Are there special challenges to these business practices?
- Are there different ways to achieve the business goal that brings a smaller compliance burden?
Scope Reduction (Outsource)

Q: Hey, doesn’t outsourcing make PCI go away???

A: You can’t outsource everything no matter what

Not that outsourcing is bad, but it doesn’t make PCI go away

In version 3.x of PCI-DSS, see:

- “Outside Service Providers”
- Requirement 12.8.2
- Requirement 12.8.5, “Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.”
Scope Reduction (P2PE)

- Awesome, but for card-present only.
- Reduces scope.
- Lets you use SAQ P2PE-HW (much smaller list of requirements).
- Integration issues.
- Your hardware needs to be certified by the PCI SSC.
- Forklift —> big investment.
- Plus side, most of this hardware supports NFC as well as mandated chip-and-PIN/chip-and-sig.
Elements of a PCI Compliance Effort

- It is far-reaching and cross-departmental.
- It is subject to interpretation.
- It can get you in big trouble if you do it wrong.
- You must approach simplifying the process logically and justify your conclusions with facts.
- Security folks should balance the compliance with improving security as well. If you focus solely on compliance, you aren't improving security.
Therefore You Should...

- Be ad-hoc ✗
- Be checklist-oriented ✗
- Run it via the standard higher ed “committee” ✗
- Be institution-wide ✓
- Be highly organized ✓
- Be project oriented ✓
- Build for a long-term ongoing effort ✓

You need (gasp!) – a FRAMEWORK!
OK, Smartie, What’s a “Framework”?

- Governance and Policy.
- Process and Procedure.
- Oversight and Authority.
Governance and Policy

- Centralized vs. Distributed
- Who attests for compliance?
- Who solves conflict or ambiguity?
- Where and how are “the rules” dictated?
Process and Procedure

- How do you get a new MID? Who can do so?
- How do you process credit cards?
- What technologies and vendors can you use?
- What is your attestation process?
- Availability of centralized services.
- Scanning and penetration testing processes?
Oversight and Authority

- What is the role of Audit?
- What is the role of Security?
- What is the role of Treasury/Cash Management?
- What is left up to local business officers and what is left up to central entities?
Examples

- Cornell
  - Big and distributed.

- BC
  - Smaller and centralized.
Also Consider...

- Make sure the governance setup reflects your existing card infrastructure.
  - How are you going to do SAQs in terms of submitting one or a bunch, or aggregating a bunch yourself and submitting one?

- Governance body/entity needs to ensure that it becomes part of the campus culture and an ongoing effort.
  - PCI has a bazillion “policies” required within it.
  - Where is the overall PCI policy, and how do it and the sub-policies fit in?

- Your QSA should agree with your governance framework, if applicable.
Building a Framework

- We are going to do this “hands-on”
- See handout for details.
Other Questions

- What else would you like to explore?
Thank You!

- Daniel Adinolfi, dra1@cornell.edu
- David Escalante, david.escalante@bc.edu

EVALUATION FORM:
http://www.educause.edu/events/security-professionals-conference/2015/
pci-program-frameworks-learning-cope-compliance
Likely Trouble Areas (1)

- Source:

- Problem: 80% of the companies they look at fail interim assessments after being PCI compliant.

- 0% of breached companies are compliant over 10 years.

- This bolsters our argument that you need a framework, not a checklist.
Likely Trouble Areas (2)

- **Requirement 11 (33% pass)**
  - This was at 9% in 2012...
  - #11.2, quarterly scans, was the main culprit

- Requirement 2 (67% pass)

- Requirement 3 (62% pass)

- Requirement 6 (64% pass)

- Requirement 8 (69% pass)

- Requirement 12 (64% pass)