

PCI: Painful Compliance Imbroglia

Declan Ingram, QSA

Securus Global

- E: declan.ingram@securusglobal.com
- P: 02 9585 1455

Agenda

- Introduction
- Background
- Doing it Wrong
- Doing it Right
- PCI DSS 1.2 Update
- The Future
- Closing Remarks

Introduction

- I am assuming you are familiar with PCI
- This is not another “Oh, here are the 12 requirements of PCI” presentation (based on things you can find in 3 seconds on the internet)

Introduction (Part 2)

- This is based upon a few years of experience working with PCI.
 - What is done well
 - What is done poorly
 - Learning from the mistakes of others

Background

- Audience participation time!
- Lets have a show of hands..
 - Who handles cardholder data ?
 - Who knows what PCI is ?
 - Who is PCI compliant ?
 - Who is a QSA ?
 - Who is just waiting for lunch ?

Doing it Wrong

Doing it Wrong

- Treating PCI DSS as a purely technical standard
 - You can't be blamed for this. People start at Rq. 1 and think it's a technical standard. Its not.
 - Do yourself a favor and start with requirement 12.
 - How can you put in a new firewall when you don't have config standards?
 - How can you make your config standards without a formal policy?
 - How can you have your policy without a risk management framework?
 - Etc. Start at the top and consider your order of operations

Doing it Wrong

- Passing ownership to a technical manager
 - I've nothing against technical managers, but PCI is not a technical standard.
 - There is a very large technical component, but it must be driven by business.
 - As above, the path of least resistance is down.
 - PCI is rarely the only compliance requirement of a business. Make sure you capitalize on lessons learnt from other compliance projects.

Doing it Wrong

- Half hearted commitment
 - You can't be half pregnant, you can't be half compliant.
 - Many organisations spend too much time working out the minimum for what they can do for compliance; this is rarely a good long term approach.
 - PCI DSS Compliance is not about the minimum required for getting the banks of your back.

Doing it Wrong

- Mis-interpreting the *intent* of the standard
 - The idea is to enforce a baseline of security
 - Don't reduce your security for compliance
 - Security Vs Compliance
 - A note about network segmentation

Doing it Wrong

- Misunderstanding the notions of **VALIDATION** and **COMPLIANCE**
 - You must be compliant at all times
 - Validation is periodic, and differs according to your merchant / service provider level.
 - Very common problem

Doing it Wrong

- Ignoring the Root causes of non-compliance
 - Think about it, why isn't your organization compliant?
 - Why are your servers not all built to a secure standard?
 - Each point of non-compliance, why?
 - Is there a formal security management framework?

Doing it Wrong

- Failing to instigate a framework for continued compliance
 - Don't forget about tomorrow!
 - You have to maintain your business
 - Don't break your business to make it compliant
 - Authentication example

Doing it Wrong

- An ad-hoc / “silo” approach
 - If your card holder data environment is all over the place, you can’t silo compliance to one site / group

Doing it Wrong

- Audience participation: QSAs
 - What is a repeated problem you have seen that isn't here?

Doing it Wrong

- Audience participation: Merchants / SPs
 - What is a problem you have had that you have not seen here?

Doing it Wrong: Conclusion

- Who has picked a theme here?

Doing it Wrong: Conclusion

- Most of the issues are business issues – the technical problems are almost always easier to solve.

Doing it Right

Doing it Right

- Taking ownership of compliance at the business level
 - Top down is often the path of least resistance

Doing it Right

- Be committed to compliance
 - Consider your options up front
 - Either jump in, or don't
 - Stick to the rules, if they don't work – amend them.

Doing it Right

- Build compliance into your security management framework
(Yes, that means you need one)

Doing it Right

- Talk to your bank, demonstrate your commitment

PCI DSS 1.2 Update

PCI DSS 1.2 Update

- Many Changes
 - Mainly explanations and clarifications
 - Definitions and terms
 - Reordering for clarity
 - Don't be fooled-
 - Changes have been made to make the intent more clear
 - A small change could effect your compliance !

PCI DSS 1.2 Update

- Some more significant changes
 - 4.1.1 WEP sunset (March 09, June 10)
 - 5.1 Anti-Malware (UNIX based systems?)
 - Don't rely on the summary
 - Read the standard!

PCI DSS 1.2 Update

- How do the changes in 1.2 effect my business ?
 - Good question! It depends on how you interpreted 1.1!

The Future (and Closing Remarks)

The Future

- **The future**
 - More deadlines
 - The banks are being patent – but don't push your luck.
 - Bigger fines, and more of them
 - Organisations are being fined NOW

Closing Remarks

- What is in it for me? <story>
- PCI DSS is here to protect the card brands from the cost of fraud. They will let your business into their processing chain if you comply to their rules.

Closing Remarks (Part 2)

- Having a compromise detected
 - Very very expensive
 - Forensic investigations
 - Merchant facilities removed
 - High pressure for fast compliance
 - Think of your staff load!

Thanks !

- Questions ?
- Contact Details:
 - E: declan.ingram@securusglobal.com
 - P: 02 9585 1455