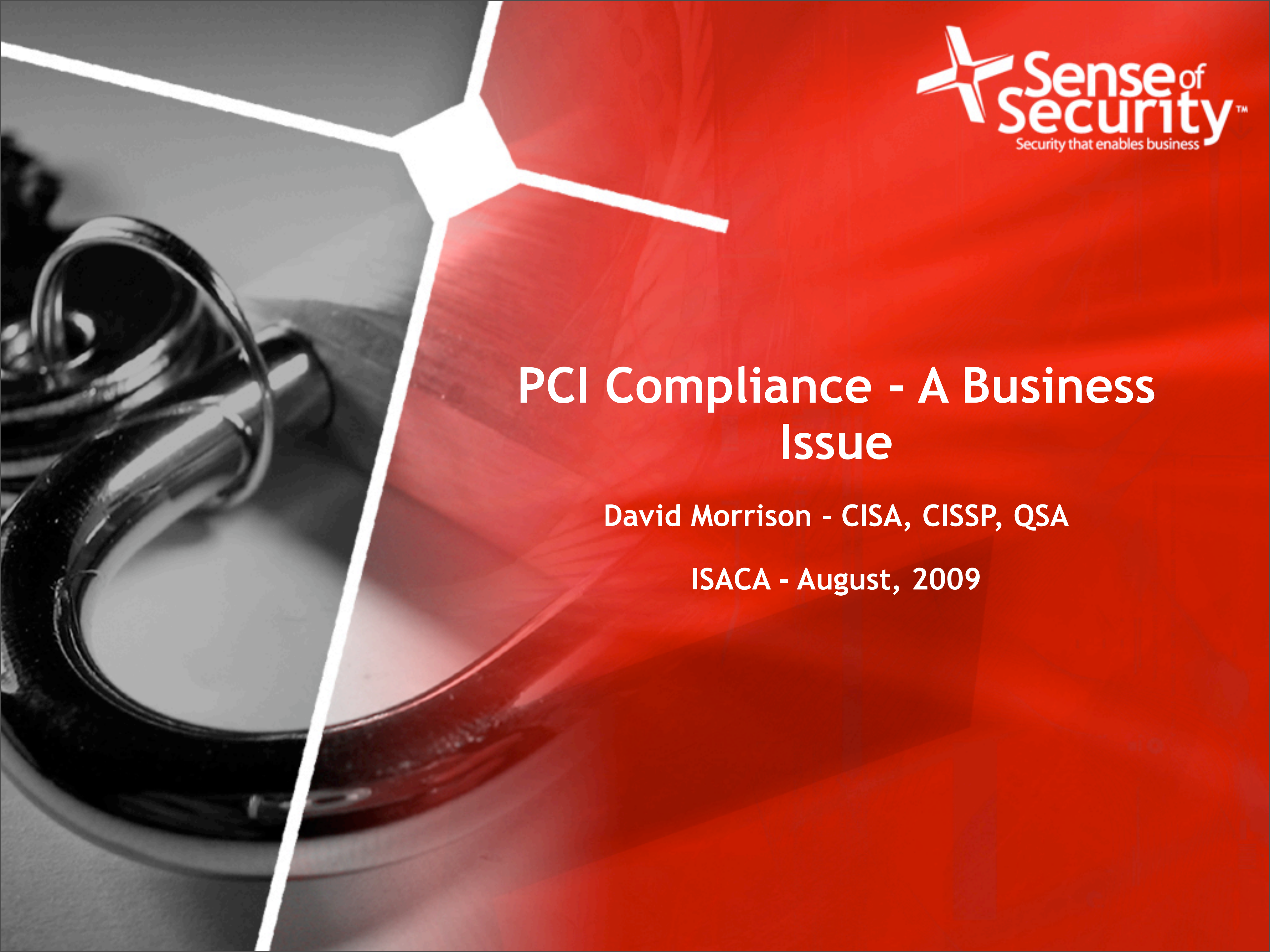

Sense of Security

Security that enables business

PCI Compliance - A Business Issue

David Morrison - CISA, CISSP, QSA

ISACA - August, 2009

Overview

1. Brief overview of PCI DSS and the associated requirements
2. Why PCI DSS is seen as an IT issue
3. What PCI DSS is really about
4. Why PCI DSS is really a business issue
5. Is outsourcing PCI DSS functions really the path to take?
6. Is PCI DSS working?
7. Conclusion

Sense of Security™
Security that enables business

PCI Data Security Standard

- Payment Card Industry Data Security Standard
  - An open industry standard
  - Developed by the founding payment brands
  - It attempts to enhance payment account data security
  - Outlines requirements for data security
  - PCI Security Standards Council (SSC) maintains a list of Qualified Security Assessors (QSAs and ASVs)
- Who must comply?
  - Everyone who stores, processes or transmits cardholder data
    - PCI compliance is mandatory
    - PCI applies to all parties in the payment process
    - An organisation may not be partially compliant: PASS or FAIL
- Merchants and Service Provider levels are based on transaction volumes

Sense of Security™
Security that enables business

PCI Compliance - An IT Issue?

Is PCI DSS an IT issue?

PCI DSS Requirements

Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security

Sense of Security™
Security that enables business

PCI Compliance - An IT Issue?

- IT based solutions will not solve all PCI DSS requirements
  - Addresses the technical requirements
  - PCI DSS is about more than just technical issues or finding technical solutions
- PCI DSS requirements should not be addressed in isolation
- Individual IT solutions create complex and unmanageable environments
- Do not believe the vendor hype, there is no silver bullet
- Manageability issues lead to security issues
- This undermines what PCI DSS is attempting to achieve

Sense of Security™
Security that enables business

The Real Requirements

- 12 Main Requirements
  - Approximately 270 Sub-Requirements

Requirement	Sub-Requirements
1	26
2	13
3	28
4	4
5	7
6	40
7	9
8	25
9	24
10	30
11	14
12	41
Appendix A (Shared Hosting Providers)	9

The Real Requirements

- From these 270 sub-requirements, some have further bullet points or sub-sub-requirements
- Not all requirements take the same time or resources. Some include entire audits, assessments or projects
- A scope of this size should not be tackled by one department alone
  - Cost
  - Resources
  - Time
- When you look deeper at these sub-requirements, they are not all IT based

Sense of Security™
Security that enables business

The Real Requirements

- Physical Security - Section 9
- Human Resources
  - 12.6 - Security Awareness
  - 12.7 - Screening of Potential Employees
- Legal Department
  - 12.8 - Legal agreements between the organisation and service providers
- All Departments
  - 12.9 Incident Response Plans

PCI DSS Complexity

- PCI Security Standards Council recognises the complexity
- Prioritised Approach Tool (PAT) released in March, 2009
  - Helps merchants and acquiring banks demonstrate and measure progress
  - Consists of 6 key milestones

1. Remove sensitive authentication data and limit data retention
2. Protect the perimeter, internal and wireless networks
3. Secure payment card applications
4. Monitor and control access to your systems
5. Protect stored cardholder data
6. Finalise remaining compliance efforts and ensure all controls are in place

Sense of Security
Security that enables business

Prioritised Approach Tool (PAT)

- Helps prioritise and target issues that cause the most harm
- The PAT has not changed the requirements. All requirements must still be satisfied
- The PAT still looks IT focused

What is PCI DSS Really About?

- PCI DSS is there to protect the card brands
- Data compromise leads to losses for the card brand
  - The card brand passes on these losses to the acquiring bank in fines
  - In most cases the acquirer passes the fine down to the offending retailer
- Financial cost of compromise
  - Fines
  - Associated costs
- Fines
  - TJX Part 1 - US$500,000 for the seriousness of the incident and impact on the VISA system
  - TJX Part 2 - US$380,000 for failure to cease storing prohibited data
- Associated Costs
  - Forrester Research suggests US$90 to US$305 per record
  - Replacement of cards
  - Credit protection
  - Legal action by card holders

Sense of Security™
Security that enables business

PCI Compliance - A Business Issue

- PCI DSS addresses business risks, not IT risks
- Data compromise affects the entire organisation
  - Financially
  - Reputation
- Requires someone that understands the business and can align PCI DSS requirements with business risks, goals and impacts
- Compliance is generally a business issue and addressed at the business level via an organisation’s overall compliance framework
  - ISO/IEC 27002
  - SOX

PCI Compliance - A Business Issue

- Why is PCI DSS addressed as a project?
- PCI DSS is not a project!
  - PCI DSS compliance does not have a start and a finishing date
  - PCI DSS is a process
  - IT is a project-based culture

PCI Security Standards Council

- PCI Security Standards Council statement on recent data breaches - 27th July, 2009
  - "Friday’s announcement of a data breach at Network Solutions underscores the necessity for ongoing vigilance of an organization’s security measures. Security doesn’t stop with PCI compliance validation. As the Council has said many times, it is not enough to validate compliance annually and not adopt security into an organization's ongoing business practices. A card data environment is under constant threat, so businesses must ensure their safeguards are also under constant vigilance, monitoring and where necessary, ongoing improvement. A layered approach to security is absolutely necessary to protect sensitive payment card data – without ongoing vigilance or a comprehensive security strategy, organizations may be just a change control away from noncompliance."

Business Support

- Requires support and backing from the business to succeed
- Requires support from those that understand the business
    - C-Level executives
    - Align PCI DSS to business risk
    - The lead for driving PCI DSS compliance should reside on the business side
- PCI DSS affects the entire organisation
    - Senior management commitment
    - Senior management remaining involved
- Resources
    - Spans departments
    - The authority to assign resources

Sense of Security™
Security that enables business

Business Support

- Policy, Process and Procedures
- Training and security awareness
- Cost
  - Compliance is not cheap
  - Business risk and costs of non-compliance far exceed implementation costs

Outsourcing PCI DSS

- No matter what the organisational size, PCI DSS is a business issue
- Whether you are level 1, 2, 3 or 4 merchant or a service provider, you must comply with all the requirements
- The only difference is how you validate your compliance, and hence the overall cost, time and resources required

Sense of Security™
Security that enables business

Outsourcing PCI DSS

- There is a common view that due to complexity and cost of addressing and remediating issues, the only solution is to outsource PCI functions
  - Four different Self Assessment Questionnaires (SAQ)
  - All PCI DSS functions outsourced allows the filing of version A of the SAQ which only covers 2 of the 12 PCI DSS requirements
  - Dial out terminal - SAQ covers 5 out of 12
  - Payment Application connected to the Internet - 11 out of 12
  - All others - All 12 requirements
- Overall cost is reduced due to the reduction in requirements
- Outsourcing does not address the underlying security issues

Outsourcing PCI DSS

- Customers are your responsibility whether you outsource or not
- You may have outsourced but you still own the problem. You are not free of compliance
- If the service provider is compromised, it is your organisation that is dragged through the mud with them
- Is the service provider you have outsourced to actually compliant?
  - Bottle Domains - April 2009
- Remember: PCI DSS compliance is only a snapshot of compliance at a single point in time

Outsourcing PCI DSS

- You cannot just rely on a Certificate of Compliance. They are not all equal.

YOU'RE COMPLIANT

This certifies that

ACME INC

Has successfully attained

PCI DSS COMPLIANCE

9 August 2009

DATE

SECRETARY

Outsourcing PCI DSS

- How far do you go in validating compliance?
  - Obtain a copy of their Certificate of Compliance (COC)
  - Obtain a copy of their Report on Compliance (ROC)
  - Assess the scope of their compliance
  - Are your systems/data stored in a compliant manner?
  - Are they willing to accept you visiting their premises?

Outsourcing PCI DSS

- PCI DSS requirements are based on security best practice
- Outsourcing does not address the underlying security issues within your organisation
- Loss of Cardholder Data is not the only issue that may affect a organisation in the event of compromise

Is PCI DSS Working?

- What about breaches that occur when a merchant or service provider is deemed PCI DSS compliant?
- Heartland Payment Systems - January 2009
  - Process payments for 250,000 businesses
  - 100 million transactions per month
  - No idea how or when the malicious software was put in place
  - Possibly effects anyone who travelled in the US in 2008
- The report is only as good as when the report was issued
- Adrian Philips, Visa's Deputy Chief Enterprise Risk Officer has stated:

> "We've never seen anyone breached that was PCI compliant. The breaches we have seen have involved a key area of non-compliance"

Is PCI DSS Working?

- PCI DSS is about security and security is an ongoing pro-active process
- How many changes are made to your environment every year?
- It is a set of guidelines to reduce risk
- Compliance can only be based on how well the QSA assesses that compliance
- We are far better off than before PCI DSS

Sense of Security™
Security that enables business

Conclusion

- PCI DSS is a business risk and cannot be solved piecemeal with IT solutions
- PCI DSS is not a project and cannot be treated as a project. It is an ongoing process that requires business support
- Outsourcing PCI DSS functions may solve compliance issues but does not address the underlying security issues PCI DSS attempts to address
- Compliance is only a snapshot in time and does not guarantee your security

Thank You

Questions?

David Morrison
Sense of Security Pty Ltd
davidm@senseofsecurity.com.au
Tel: +61 2 9290 4443
http://www.senseofsecurity.com.au

Security that enables business