

7 Things Hackers Don't Want You To Know About PCI

Bruce Sussman, CPA, CISA, CISSP

Course Objectives:

Identify the PCI DSS Standards
You Can Take to a Higher Level
And Better Protect Your Organization

Introduction

- You are not limited to the minimum or baseline controls
- PCI DSS is a consensus document
- Criminals move faster than PCI DSS standards
 - Example: Recent successful attacks on knowledge based authentication
- You can take PCI DSS to a higher level

The Dangers

1. Outdated risk assessments
2. Inadequate fraud tools and response plans
3. Lack of application firewalls
4. Software only/ proprietary encryption
5. Voice-based authentication for password resets
6. Unencrypted internal network traffic
7. More comprehensive penetration testing



#1 Danger - Outdated Risk Assessments

Vulnerabilities

- Complacency at “compliant” organizations
 - PCI DSS is a “point in time” assessment
 - Was the assessment only a “homework exercise”?
 - Reliance on breached defenses in peer organizations
 - WEP-based defenses

#1 Danger - Outdated Risk Assessments

Why Is This Important?

- You can not defend against unanticipated threats.
- Updating risk assessments shows due diligence if you are breached.
- Older risk assessments may predate newer state laws which mandate PCI compliance or card security.

#1 Danger - Outdated Risk Assessments

Other Vulnerabilities

- Some organizations don't consider securing related payment channels that fraudsters simultaneously attack.
 - ACH and remote banking application
 - Recent attacks have become ***cross channel*** and ***cross border***
 - Attacks are slowly executed over time and difficult to recognize

7 Things You Can Do

#1 Update Risk Assessments

- Look for outdated defenses
- Mandate enterprise-wide participation
- Consider next generation authentication methods and payment schemes which can mitigate risk

7 Things You Can Do

#1 Update Risk Assessments

Next Generation Payment Technologies

- Encryption and/or data disguising traffic from POS terminal to network (several variants,
- Review ASC X9 standardization effort
- Chip and PIN (full EMV)
- Magnetic stripe fingerprinting

7 Things You Can Do

#1 Update Risk Assessments

- One time alternate card number
- Strengthening user authentication (Biometric, One Time Password token)
- Contactless: Unique Payment UPIC/ Pseudo PAN

7 Things You Can Do

#1 Update Risk Assessments

- Assess the control maturity of your organization
- Consider the following methodology:
- (used with permission from the BITS Third Party Risk Committee)

Payments Risk Competency Framework May Inform PCI Assessments

Revised Payments Risk Competency Framework

Payments Risk Competency Level	Skills and Expertise	Awareness and Communication	Governance, Policies, Standards and Procedures	Risk Tools, Measurement, and Analysis	Audit and Competency Level Assessment
Level 1: Initial	Skills required for effective payments risk mitigation are not identified. A training plan does not exist and no formal training occurs.	Recognition of the need for the payments risk mitigation process is emerging. There is sporadic communication of the issues.	There are ad hoc approaches to payments risk mitigation processes and practices. The processes and policies are not consistently defined. There is no oversight of payment product risk or performance.	No systemic processes exist to measure the source, magnitude and direction of payments risk, either from new or legacy products or services. Some desktop based risk mitigation tools may exist, on a one-off basis. Management is unaware of the cost of compliance vs. the risk of inaction.	Independent assurance over key business and technical processes is not performed. Competency level assessment: Self
Level 2: Repeatable but Siloed and Intuitive	Minimum skill requirements for effective payments mitigation are identified for critical areas. Training is provided in response to needs or events, rather than on the basis of an agreed plan, and informal training on the job occurs.	There is awareness of the need to act. Management has begun to communicate regularly on payment system risk mitigation issues. Communication addressing payments risk issues occurs within individual organizational structures, but not between silos.	A consistent set of risk mitigation processes begins to emerge, but are largely intuitive. Some aspects of the process are repeatable because of individual expertise and some documentation. Informal understanding of policies and procedures may exist. There is an informal group that meets occasionally to address specific payments loss events and designs specific risk mitigation procedures to address these events.	Management begins to reactively assess payments risk inherent to existing operations, products and services. A knowledge base of payments risk and common approaches to the use of payments risk mitigation tools exist and accrues to those who produce the initial assessments but it is not well understood outside of the local project team. Vendor tools may have been acquired, but are probably not applied correctly, and may even have not been used or properly implemented.	Management and the Board are aware that external stakeholders (key customers, regulators, investors) require independent assurance. However, there is little perceived value in independent audit until it becomes mandatory. Competency level assessment: Internal, more formal
Level 3: Defined Process	Skills requirements, including the development of a payments risk mitigation common body of knowledge, are defined and documented for all areas. A formal training plan has been developed, but formal training is based on individual initiative.	There is understanding of the need to act. Management effectively communicates the overall issues, including those arising from changes to payment network rules, new or revised regulatory guidance, technology trends, etc. Effective communication occurs within and across organizational lines regarding payments issues.	Use of good practices has emerged. Payments risk mitigation processes, policies and procedures are appropriately defined and documented for all key activities. Formal understanding of policies and procedures exists. A standing Payments Committee with representatives from major payment channels exists. Specific loss events are evaluated for root cause and risk mitigation procedures are developed. Payments risk and performance metrics are reported and trends are monitored.	Management begins to proactively develop payments risk tolerances, limits, policies, procedures and objectives. A plan has been defined for use and tools have been standardized to automate the payments risk mitigation process for basic purposes. Formal responsibility for measuring and reporting risk is assigned. Ad hoc tools are used to acquire data used for risk management but may not all be in accordance with the agreed plan, and may not be integrated with one another.	Management becomes acclimated to the requirements (frequency, issues, documentation request) of independent auditors. Management begins to allocate internal resources to hire internal auditors, payments risk management specialists, and to codify key policies. The organization begins to think "what will the auditors" say. Competency level assessment: Independent audit
Level 4: Managed and Measurable	Skills requirements are routinely updated for all areas, proficiency is ensured for all critical areas and certification is encouraged. Mature training techniques are applied according to the training plan and knowledge sharing is encouraged. All internal payments risk mitigation experts are involved and the effectiveness of the training plan is assessed.	There is understanding of the full set of payments risk mitigation requirements and the need to keep staff current about material changes that could impact the payments business. Mature communication techniques are applied within and across organizational lines and standard communication tools are in use. Feedback from customer-facing associates and backroom operational associates is captured and acted upon in a timely manner. Policy exceptions are identified and reported to the Payments Committee.	Payments risk mitigation process is sound and complete; internal best practices are applied across multiple areas of the business. All aspects of the process are documented and repeatable. Policies have been approved and signed off by management, including the board of directors. Standards for developing and maintaining the processes and procedures are adopted and followed. Periodic review is required. A Payments Committee with representatives of all payments channels exists. Payments risk and performance metrics are reported and trends are monitored. The company metrics are compared to peer benchmarks and/or payment brand metrics.	Formal metrics are reliable, disseminated, and used to manage tolerable payments risk. Data analysis tools evolve from ad hoc to either off the shelf or robust in-house solutions, and some have been integrated with other related tools. A wide range of payments risk mitigation techniques are used, with appropriate actions taken by management on a timely basis. The FI has begun to benchmark itself against industry performance metrics. Processes for capturing new types of payments risk are reliable and extended before entry into new businesses or association with new partners.	Internal audit and risk management are viewed as partners with management in sensible risk taking and in payments risk avoidance. Management policies and board committee documents clearly indicate that management is ultimately responsible for limiting risk and for controlling operative risk management policies and that effective practices are in place. Competency level assessment: External audit
Level 5: Optimized	Continuous improvement of skills, based on clearly defined personal and organizational goals, is encouraged. Training and education support external best practices and use of leading edge payments risk mitigation concepts and techniques. Professional certification is required for key positions. Knowledge sharing is an enterprise culture and knowledge-based risk mitigation systems are being deployed. External experts and industry leaders are used for guidance.	There is forward-looking understanding of payments risk mitigation requirements. Proactive communication of issues based on trends exists, mature communication techniques are applied within and across organizational lines and integrated communication tools are in use. Policy exceptions are identified by automated systems that allow action to be taken to effectively mitigate risk. Exceptions are reported to the Senior Management Committee.	External best practices and standards are applied. Process documentation is evolved to automated workflow. Processes, policies and procedures are standardized and integrated to enable end-to-end management and improvement. There is payment product oversight by a Senior Management Committee that meets regularly to proactively address risk in new payment products, review key payments risk and performance metrics and set payment risk appetite.	Payments risk management metrics increase in number and sophistication, and may include online or real time tools. These tools are fully integrated across the enterprise to enable end-to-end support of the processes. Enterprise wide monitoring and issue remediation is in place and as a result the FI has the ability to monitor transactions seamlessly across channels. The FI routinely benchmarks against industry performance metrics and typically excels. A portfolio approach is used to identify and aggregate enterprise-level cross channel payments risks. The entity is completely up to date with both regulatory requirements and any relevant regulatory guidance	Internal audit and payments risk management practices are enterprise wide, repeatable and not dependent on key personnel or favorable business conditions. Audit tools and procedures reliably evolve and forecast over the horizon risks. Continuous monitoring is routine. Competency level assessment: External certified risk based audit

Slide 12

CDS2

What would we plan to with this slide....

Craig Sullivan, 4/13/2010

Situation Analysis

Both processors have just passed their most recent annual PCI DSS examinations.

Processor A

- Mid-sized regional payments processor
- Handles retail payments applications at about 2500 merchants, which together have about retail 10,000 physical locations
- Installs and drives POS terminals which process PIN and Signature debit and credit card transactions
- Processes checks, and converts them to either ACH or image transactions based upon the agreements merchants have with financial institutions
- Has a domestic-only Internet business, where it handles about 300 additional online merchants
 - Some of these Internet merchants might be considered high risk
- Is a gateway to all major networks, both ACH processors, and has sponsoring relationships with about 300 financial institutions

Processor B

- Mid-sized regional payments processor, but it has an international Internet business
- Handles retail payments applications at about 2200 merchants, which together have about 7,500 retail physical locations
- Installs and drives POS terminals which process PIN and Signature debit and credit card transactions
- Processes checks, and converts them to either ACH or image transactions based upon the agreements merchants have with financial institutions
- Has a smaller Internet business, but some of its merchants are based offshore
 - Some of these Internet merchants might be characterized as high risk
- Is a gateway to all major networks, both ACH processors, and has sponsoring relationships with about 270 financial institutions

Situation Analysis

Additional Background

Processor A

- Initially failed its PCI examination one year ago. Management recognized that the company's risk mitigation capabilities and culture were inadequate to withstand an increasingly threatening risk environment. At the direction of its Board, the company:
 - Replaced its Chief Risk Officer, and the CEO reorganized its risk and IT staff to better manage emerging threats. The reorganization was completed about six months before its most recent PCI exam.
 - Installed a comprehensive set of the latest detection and mitigation tools, and keeps the CEO's risk working group (which meets monthly) informed of any and all risk related events.
 - Began to benchmark its security operation against industry best practices.
 - Evaluated its physical security environment and made a significant investment in the processor's 3 physical facilities, now underway.

Processor B

- Has passed all of its PCI DSS examinations. There have been intermittent risk issues over the last decade, but none have been headline events. The company's:
 - Senior risk mitigation staff has been in place for about a decade with little turnover.
 - IT and risk structure has not changed materially in the last 5 years.
 - CIO and CSO report to the Chief Operations Officer, who reports to the President.
 - Organization includes no standing risk or security committee.
 - Tools and procedures are upgraded on an ad hoc basis, usually in response to specific security events.
 - Benchmarking is irregular.
 - Operations are housed at 2 physical facilities, one about 12 years old and the second about six years old. Those facilities are upgraded on an ad hoc, as required, basis.

Situation Analysis

Analysis Suggests Processor B Is At Higher Sustained Noncompliance Risk

Governance, Policies, Standards and Procedures Yardstick With Firm Assessment

Assessment Factors – Governance, Policies, Standards and Procedures	Processor A	Processor B
Governance		
No or irregular management oversight occurs	5	2
A management oversight committee exists with cross-functional membership	5	2
Formal reporting of key risk and performance indicators is provided to senior management and the Board	4	3
Policies		
Informal policies and procedures exist	4	4
Written policies exist	5	3
The Board has approved the policies	4	2
Policies are reviewed and updated on a regular basis	5	3
Reporting of policy exceptions occurs and trends are analyzed	3	2
Standards and Procedures		
Processes and procedures are not standard and variances exist	4	2
Risk mitigation processes and procedures are documented and followed	4	3
Key risk and performance metrics are compared to peer benchmarks	4	2
Best practices have been adopted and risk mitigation processes are efficient and effective	4	3

Risk Competency Level:

Processor A: Level 4

Processor B: Level 2

Continuity Assessment:

Processor A: 4.2

Processor B: 2.51



#2 Danger - Inadequate Incident Plans and Fraud Management

Vulnerabilities

- Fraud response plans without real time alerts
- Relying on transaction logging alone
- Relying only on your vendor for fraud detection or their IDS/IPS
- No information sharing capability with peers or law enforcement

#2 Danger - Inadequate Incident Plans and Fraud Management

Why Is This Important?

- Card association/ network rules require use of fraud management tools.
- Point of compromise and point of fraud correlation are becoming more difficult
 - Card frauding marketplaces mask source and use of stolen card data.

7 Things You Can Do

#2 Improved Fraud Detection

- Implement fraud management tools which:
 - Recognize fraud pattern in real time at the card and platform level.
 - Leverage information sharing.
- Maintain internal tools.
- Update of signature based fraud rules, and malware/ virus signatures.

#3 Danger - Lack of Application Firewalls

Vulnerabilities

- Malware attacks exploit SSL/ HTTPS and send malware to your application
- Avoid MSP over-reliance
 - Did you ask IDS providers/ MSPs about using application level firewalls?
 - Purchase your own?
 - Understand the capabilities of their respective solutions.



7 Things You Can Do

#3 Implement Application Level Firewalls

Why Is This Important?

- This is an optional control PCI DSS 6.6 Question 6 (alternate procedure is a code review).
- Some organizations rely on network-level firewalls.
- Network-level firewalls and MSPs ***do not always*** see encrypted malware.



#4 Danger - Software Only/ Proprietary Encryption

Vulnerabilities

- Software encryption is vulnerable to decryption utilities and commands.
- Some organizations do not protect or rotate encryption keys.
- What if the vendor uses algorithms which have not been reviewed independently?

#4 Danger - Software Only/ Proprietary Encryption

Why Is This Important?

- Some organizations using software only or proprietary encryption may be exposed when:
 - Encryption key custodians leave.
 - The application is upgraded.
 - A suspected compromise occurs.
 - A key becomes corrupted and needs to be replaced.

7 Things You Can Do

#4 Upgrade Your Encryption Key Management

- Always understand the encryption application you have purchased.
- Tightly control utilities which unmask or decrypt keys.
- Scrutinize proprietary encryption solutions.
- Use Hardware Security Modules (HSM).
 - Lock down your HSM and remove high risk commands.

7 Things You Can Do

#4 Upgrade Your Encryption Key Management

Merchants and Servicers

- Use Hardware Security Modules (HSM).
- Consider end-to-end encryption.
- Change encryption keys more frequently.
- Upgrade payment applications to most recent PA DSS levels.

Issuers

- Reissue payment cards when keys are suspected of compromise
- Consider Chip and PIN cards

#5 Danger - Using Voice-Based Authentication for Password Resets

Why Is This Important?

- Using voice based authentication for password resets creates exposure to social engineering.

Vulnerabilities

- Voice based authentication does not scale well to medium/ large organizations.
- Not specifically prohibited by PCI.
- Procedure is vulnerable to mistakes and spoofing.

7 Things You Can Do

#5 Replace Voice-Based Authentication

Consider these steps:

- Utilize challenge response devices.
- Implement out of band authentication of password reset requests.
- Multiple layers of authentication.

#6 Danger - Unencrypted Internal Network Traffic

Vulnerabilities

- Insider abuse of authorized access.
- Undetected network intrusion.
- Rogue wireless connections.
- Surreptitious network attached devices
- MPLS and unencrypted private carrier networks

7 Things You Can Do

#6 Encrypt Sensitive Internal Network Traffic

Why Is This Important?

- Encrypting internal network traffic compensates for unknown data leakage.
- Creates defense in depth.
Behind the firewall isn't always private.
- Encrypt internal traffic carrying card data with at least SSL v2 or equivalent.

#7 Danger - More Comprehensive Penetration Testing

Vulnerabilities

- PCI DSS Requirement #11 does not mandate testing for weaknesses in employee security awareness
 - Emails/ Phishing.
 - The “friendly” visitor.

7 Things You Can Do

#7 Better Penetration Testing

Why Is This Important?

- Employees are subject to trickery and deception.
- Test the human factor and safeguard social engineering and trickery.
 - Perform penetration tests more frequently than annually.
 - Consider Data Leak Protection (DLP) tools.

Let's Review the 7 Things You Can Do

1. Update Risk Assessments.
2. Improve Incident Plans & Fraud Detection & Management.
3. Utilize Application Firewalls.
4. Upgrade Your Encryption Key Management.
5. Better authenticate Password Resets.
6. Encrypt Sensitive Internal Network Traffic.
7. Improve Penetration Testing.

Closing Thoughts

...compensating controls can be a double-edged sword

- Adversaries can sometimes guess the payment application vulnerabilities.
- Should exceed the PCI requirement.
- Do not over use them.

Closing Thoughts

Don't mistake "compliant" for "secure"

- PCI compliance is measured as a point in time.
- Vulnerabilities and the capabilities of adversaries improve over time.
- Go above and beyond

Don't Forget The Dangers

1. Outdated risk assessments
2. Inadequate fraud tools and response plans
3. Lack of application firewalls
4. Software only/ proprietary encryption
5. Weak user authentication
6. Unencrypted internal network traffic
7. More comprehensive penetration testing





Thank you!

www.crowehorwath.com

Bruce.Sussman@crowehorwath.com

973.422.7151

