


www.coresecurity.com



## Security Testing: The Easiest Part of PCI Certification


Core Security Technologies  
September 6, 2007

www.coresecurity.com



## Agenda

- The PCI Standard: Security Basics and Compliance Challenges
- Compliance + Validation = PCI Certification
- PCI Requirements for Security Testing
- CORE IMPACT – How It Helps with PCI Certification
- Customer Case Study
- PCI Deadlines and Clarifications – Why You Should Care Now
- Next Steps & Questions



## About the Speaker



[www.coresecurity.com](http://www.coresecurity.com)

### About Tom Kellermann

- VP, Security Awareness
- Represents Core in government and industry security working groups
- Certified Information Security Manager (CISM)
- Previously Senior Data Risk Management Specialist for the Treasury of the World Bank
- Co-author of “E-safety and Soundness: Securing Finance in a New Age,” “E-security: Risk Mitigation in Financial Transactions” and “Mobile Risk Management”

## Security Basics and Compliance Challenges



[www.coresecurity.com](http://www.coresecurity.com)

### PCI Standard Recap: It's Basic Security

- Keep customer records secure as merchants and processors store, transmit and manage credit and debit card data.
- Mandates basic security best practices that include implementing and ensuring the effectiveness of:
  - Firewalls
  - Passwords and other security parameters
  - Encryption and other data protection measures
  - Anti-virus applications
  - Security patches
  - Data access control and tracking measures
  - Security testing applications, including scanning and pen testing
  - IPS, IDS and other defensive applications
  - End-user awareness and incident-response programs
- A diligent company that makes proper use of security defenses and implements basic security policies can meet most of the requirements prior to even reviewing itself for PCI compliance.

### Easier said than done?

- There's a lot to do
- Some guidelines are phrased in a confusing fashion
- Interpretation is often up for debate, particularly among audit firms
- Multiple levels of merchants and service providers
- Confusion about who is responsible for doing what



### Where's the low-hanging fruit?

- Testing security defenses and end-user security awareness is one of the easiest things you can do to comply with and validate a broad swath of PCI requirements.

### Compliance vs. Validation

- Merchant Level II? Service Provider Level 1? ...There is no difference in compliance requirements.
- The confusion is between *compliance* and *validation*.
  - Compliance
    - » Implementing the security measures and policies outlined in the Standard
  - Validation
    - » Proving that you are compliant
- You must do BOTH to achieve PCI certification



## Visa PCI Validation Requirements

Merchant Level	Service Provider Level	Validation Requirements		
		Annual On-Site PCI Assessment by a QSA (or internal if signed by officer)	Annual PCI Self-Assessment Questionnaire	Quarterly Network Scan by an ASV
1	1 & 2	✓		✓
2, 3 & 4*	3		✓	✓

- Notes for Merchants:
  - Any merchant that has an account data compromise may be escalated to Level 1.
  - Compliance validation is required for Level 1, 2 and 3 merchants, and may be required for Level 4 merchants.
  - \*Specific validation requirements for Level 4 vendors are set by the acquiring banks.

Self Assessment ...

... or Third-Party Assessment

**Build and Maintain a Secure Network**

*Requirement 1: Install and maintain a firewall configuration to protect data*

DESCRIPTION	RESPONSE
1.1 Are all router, switches, wireless access points, and firewall configurations secured and do they conform to documented security standards?	<input type="checkbox"/> Yes <input type="checkbox"/> No
1.2 If wireless technology is used, is the access to the network limited to authorized devices?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
1.3 Do changes to the firewall need authorization and are the changes logged?	<input type="checkbox"/> Yes <input type="checkbox"/> No
1.4 Is a firewall used to protect the network and limit traffic to that which is required to conduct business?	<input type="checkbox"/> Yes <input type="checkbox"/> No
1.5 Are egress and ingress filters installed on all border routers to prevent impersonation with spoofed IP addresses?	<input type="checkbox"/> Yes <input type="checkbox"/> No



- Either way, you need to confirm that your defensive infrastructure and security policies are in-place and working.
- In both cases, performing your own security testing – and specifically penetration testing – helps with compliance and validation.

## PCI Requirements for Security Testing



www.coresecurity.com

Security assurance (aka testing and proving) permeates the PCI Standard – over 40 occurrences of “test,” “ensure” and “assure.”

- **Requirement 1: Firewalls**

- 1.1.1 Test network connections and firewall changes.

- **Requirement 2: System passwords and security parameters**

- 2.2 Assure that system configuration standards address vulnerabilities.

- **Requirement 5: Anti-virus software**

- 5.1.1 Ensure that anti-virus programs can detect, remove, and protect against malware.

- 5.2 Ensure that anti-virus mechanisms are current, running, and generating audit logs.

- **Requirement 6: Secure systems and applications**

- 6.1 Ensure that system components and software have the latest security patches.

- 6.3.1 Test all security patches and system and software configuration changes.



## PCI Requirements for Security Testing



www.coresecurity.com

- **Requirement 11: Regularly test security systems and processes**

- 11.1 Test security controls, limitations, network connections, and restrictions to assure the ability identify and stop unauthorized access attempts.

- 11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network.

- 11.3 Perform penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).

- 11.4 Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines up-to-date.

- **Requirement 12: Maintain an end-user information security policy**

- 12.9.2 Implement an incident response plan and test it annually.



## CORE IMPACT: Automated Penetration Testing

- Safely test your systems, end users and end-user applications against real-world data breach attempts – see your security from an attacker’s point of view.
  - identify real vulnerabilities in operating systems and OS services
  - measure end-user response to social engineering attacks
  - test and tune information security defensive infrastructure
  - validate the security of system upgrades, modifications and patches
  - establish an audit trail of your vulnerability management practices
- Evaluate security defenses and policies – on an ongoing basis – with Rapid Penetration Tests (RPT) that integrate pen testing best practices into a wizard-driven interface.
- Full reporting and audit trails provide info required by PCI auditors.



## How IMPACT helps with PCI

- IMPACT allows you to “test,” “ensure” and “assure” the effectiveness of all the security defenses and policies in the requirements we mentioned previously ...



## How IMPACT helps with PCI

### **Requirement 1: Install and maintain a firewall configuration to protect cardholder data**

1.1.1 Establish firewall configuration standards that include a formal process for approving and testing all external network connections and changes to the firewall configuration.

*(IMPACT assists with Reqs 1.2 and 1.3 as well)*



## How IMPACT helps with PCI

### **Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters**

2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards ...



## How IMPACT helps with PCI

### Requirement 5: Use and regularly update anti-virus software or programs

5.1.1 Ensure that anti-virus programs are capable of detecting, removing, and protecting against other forms of malicious software, including spyware and adware.

5.2 Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.



## How IMPACT helps with PCI

### Requirement 6: Develop and maintain secure systems and applications

6.1 Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.

6.3.1 Test all security patches and system and software configuration changes before deployment

*(IMPACT also assists with Req 6.2)*



## How IMPACT helps with PCI

### Requirement 11: Regularly test security systems and processes

11.1 Test security controls, limitations, network connections, and restrictions annually to assure the ability to adequately identify and to stop any unauthorized access attempts ...

11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).



## How IMPACT helps with PCI

### Requirement 11: Regularly test security systems and processes

11.3 Perform penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).



## How IMPACT helps with PCI

### Requirement 11: Regularly test security systems and processes

11.4 Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines up-to-date.



## How IMPACT helps with PCI

### Requirement 12: Maintain a policy that addresses information security for employees and contractors

12.6 Implement a formal security awareness program to make all employees aware of the importance of cardholder data security.

12.9.2 Implement an incident response plan and test it annually.



## How IMPACT helps with PCI

- It also tests a number of other things that the Standard implicitly assumes should be tested and effective, such as:
  - the cardholder data access restriction (section 7)
  - tracking and monitoring mandates (section 10)



## Customer Case Study

### Case Study: Level 2 Merchant Seeking Security Testing Solution for PCI

- Processes millions of card transactions per year
- IT Security Manager wanted a way to verify his company's security posture and determine where vulnerabilities were and how they could be compromised - and to help determine how to fix weaknesses.
- Specifically, he wanted to:
  - validate and confirm the vulnerabilities identified in GFI LANGuard network scans
  - verify that the company's anti-virus solutions are working
  - confirm that the latest OS patches are in-place
  - get metrics on end-user security awareness
  - test the functionality of their intrusion prevention system



### Other pen testing options

- He considered bringing in third-party consultants, but he wanted to ...
  - ... keep test results “in the family” – IT people are often apprehensive about revealing security weaknesses outside the organization
  - ... test regularly to stay on top of infrastructure changes and ahead of new threats
- He considered manual testing using publicly available exploits, but ...
  - ... “Downloading exploits off the Internet isn’t exactly the most responsible thing to do.”
  - ... he needed a commercial solution



### Justification

- He saw PCI as an easy way to justify the purchase of something that he “needed to do anyway,” (in his words) since pen testing directly fulfills requirement 11.3 and supports compliance with many other requirements
- By helping him prevent data breaches, the product would also help his company maintain the company’s level 2 merchant status.
  - If the company suffered a breach, they would likely be moved to Level 1 and have to undergo annual on-site PCI assessments (in addition to incurring financial penalties).



## Customer Case Study



www.coresecurity.com

### Business Case

- Fulfillment of PCI requirements / Help prevent data breaches
- Commercial-grade product that's developed by professionals
- All exploits are thoroughly tested, guaranteed to be safe, and regularly updated
- Used by hundreds of major organizations and government agencies
- Recommended by people at conferences he attended
- For auditors: a clear, complete record of his testing practices and proof that security measures are working
- Rapid Penetration Tests would allow self-sufficient testing without extra staff
- "It was a no-brainer"



## Why You Need to Care Now



www.coresecurity.com

### Upcoming deadlines and fines

- Acquiring banks that fail to ensure compliance by Sept. 30, 2007 will be assessed fines starting at \$5,000 a month for each noncompliant merchant.
- The fines increase to \$25,000 per month for each noncompliant merchant after Dec. 31, 2007.

### Who is responsible for what

- Acquiring banks (financial institutions that grant retailers and other entities the approval they need to accept credit cards) are responsible for ensuring that merchants comply with the standard and that the merchants use service providers that comply.
- Acquiring banks are bound by the compliance validation dates and face penalties for missed deadlines and non-compliant merchants.
- *If you are a merchant, your acquiring bank will most likely pass these penalties on to you.*



## Why You Need to Care Now



www.coresecurity.com

### The Interchange Rate Penalty

- Oct. 1, 2007: non-compliant merchants will no longer qualify for the best available tiered interchange rates from Visa.
- Interchange rates apply to each transaction and is paid to card issuers by acquirers, which ordinarily pass the fees to merchants with a markup.
- Visa and Interlink transactions submitted by noncompliant merchants will be downgraded one interchange tier starting October 1.



## Why You Need to Care Now



www.coresecurity.com

### The Interchange Rate Penalty: Effect on Profits of a Billion-Dollar Company

- Reduction in profits from *debit card* transactions
  - Current Tier 1 interchange rate: .62%
  - New rate for non-compliant merchants: .81%
  - Profit reduction for a billion-dollar company (33% of transactions being debit card-based): **\$627,000 per year**
- Reduction in profits from *credit card* transactions
  - Current Tier 1 interchange rate: 1.43%
  - New rate for non-compliant merchants: 1.47%
  - Profit reduction for a billion-dollar company (33% of transactions being credit card-based): **\$132,000 per year**
- Total Profit Reduction: **\$759,000 per year**
  - Would reduce a 6% overall profit to 4.735% (doesn't incl. other fines)



# Recognition

[www.coresecurity.com](http://www.coresecurity.com)

---

**informat.com** "We have reviewed, tested, and played with many products and applications over the years, but none of them compare to CORE IMPACT."  
- informat.com, May 4, 2007

**ISSA** "CORE IMPACT was a blast to test and a product I am certain would benefit organizations that choose to engage it."  
- ISSA, May 4, 2007

**Hotpick** "CORE IMPACT 6.0 is an amazing tool to validate your security posture."  
- Information Security Magazine, January 16, 2007

**WINNER** "We rate CORE IMPACT as Lab Approved ... and we will be adding it to our test bench for the coming year."  
- SC Magazine, January 7, 2007

Wall Street Journal Technology and Innovation Award: Runner-Up, IT Security and Privacy  
- September 2006

eWeek Excellence Awards: Vulnerability Assessment and Remediation – May 2006

"After using IMPACT it seems obvious to us that manual penetration is obsolete."  
By Earl Geer

"Organizations concerned with maintaining a tight security profile will appreciate Core Security Technologies' CORE IMPACT 6..."  
By Cameron Sturdevant

Info Security Hot Company – February 2006

# Sample IMPACT Customers


**Banking and Financial Services**

**Retail**


**Media / Entertainment / Travel**


**Manufacturing**


## Sample IMPACT Customers




**Federal / State / Local Government**




**Energy and Utilities**


**Professional Services**



**Telecommunications**




## Sample IMPACT Customers




**Technology**



**Healthcare**



**Education**



## Next Steps

[www.coresecurity.com](http://www.coresecurity.com)



- See a CORE IMPACT demonstration
  - Enter your **name, company, email and phone** in the Webex question window if you'd like to see a product demo.
- Get more information about Security Testing and PCI
  - All attendees will receive links to a “Security Testing for PCI” resources kit and a recorded version of this webcast.



## Questions

[www.coresecurity.com](http://www.coresecurity.com)



- Any questions?
- Contact us:
  - Tom Kellermann, VP of Security Awareness  
[tom.kellermann@coresecurity.com](mailto:tom.kellermann@coresecurity.com)
  - Mike Yaffe, Director of Product Marketing  
[mike.yaffe@coresecurity.com](mailto:mike.yaffe@coresecurity.com)
  - Phone: +1 (617) 399-6980  
[www.coresecurity.com](http://www.coresecurity.com)

