



PCI Compliance **Overview**

Section **6.6** Dissected and Elaborated

September 2008

- Purpose
 - Help prevent theft of consumers' data
- Motivation
 - Security breaches
 - Need for more prescriptive guidelines than prior regulations
- Participants
 - American Express - Data Security Operating Policy (DSOP)
 - Discover - Discover Information Security and Compliance (DISC),
 - MasterCard Site Data Protection (SDP) and
 - Visa - Cardholder Information Security Program (CISP)
- Applies to:
 - Any business that accepts credit cards needs to be aware of the PCI Data Security Standards and implement them on its network.

- 1980s was all about desktop security with viruses
- 1990s saw the advent of network and by early 2000s, Internet e-commerce was starting to boom...
- Along with the hackers who started having a field day through the network and then through Web applications – credit card fraud reached over \$1B
- Each of the major card companies (Amex, Discover, JCB, MC, VISA) had their own standard
- MC created the Payment Card Industry (standard) which the other companies agreed to in 2004 and the regulation went into effective on June 30, 2005
- PCI Standard was updated in September 2006 to Version 1.1
- Clarification to Sections 6.6 (App security) and 11.3 (Pen testing) issued in April, 2008

- **PCI Data Security Standard (PCI DSS) applies to merchants and third-party service providers that store, process or transmit credit card/debit card data**
- **Twelve requirements:**
 - Build and Maintain a Secure Network
 - Requirement 1: Install and maintain a firewall configuration to protect cardholder data
 - Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
 - Protect Cardholder Data
 - Requirement 3: Protect stored cardholder data
 - Requirement 4: Encrypt transmission of cardholder data across open, public networks
 - Maintain a Vulnerability Management Program
 - Requirement 5: Use and regularly update anti-virus software
 - Requirement 6: Develop and maintain secure systems and applications

- **Twelve requirements (continued):**
 - Implement Strong Access Control Measures
 - Requirement 7: Restrict access to cardholder data by business need-to-know
 - Requirement 8: Assign a unique ID to each person with computer access
 - Requirement 9: Restrict physical access to cardholder data
 - Regularly Monitor and Test Networks
 - Requirement 10: Track and monitor all access to network resources and cardholder data
 - Requirement 11: Regularly test security systems and processes
 - Maintain an Information Security Policy
 - Requirement 12: Maintain a policy that addresses information security
- **Failure to comply with even 1 requirement results in non-compliance**
- **Acquirers and ISOs are also required to ensure that their merchants are compliant**

Merchant Categories



Merchant Level	Criteria	Requirements
Level 1	<ul style="list-style-type: none">▪ Over 6M transactions a year; or▪ Merchants whose security has been violated	<ul style="list-style-type: none">▪ Annual onsite review by merchant's internal auditor or a Qualified Security Assessor (QSA), or▪ Internal Audit, and a quarterly network security scan with an Approved Scanning Vendor (ASV)
Level 2	<ul style="list-style-type: none">▪ 1M to 6M Transactions	<ul style="list-style-type: none">▪ Completion of PCI DSS Self Assessment Questionnaire annually, and quarterly network security scan with an approved ASV
Level 3	<ul style="list-style-type: none">▪ 20,000 to 1M Transactions	<ul style="list-style-type: none">▪ Completion of PCI DSS Self Assessment Questionnaire annually, and quarterly network security scan with an approved ASV
Level 4	<ul style="list-style-type: none">▪ Less than 20,000 Transactions	<ul style="list-style-type: none">▪ Completion of PCI DSS Self Assessment Questionnaire annually, and quarterly network security scan with an approved ASV

- **Merchants** – Conduct business online to sell their merchandize
- **Service providers** – Used by Merchants for all kinds of services including selling content online, payment services, hosting applications and processing
- **Independent Sales Organization (ISO)** – Sells a Bank's services, can mark-up and sign merchants
- **Acquirer** – An acquiring bank which maintains merchant relationships and receives all bankcard transactions from the merchant
- **QSA** – Qualified Security Assessor - provides services to payment application vendors in order to validate such vendors' payment applications as adhering to the requirements of the PA-DSS
- **ASV** – Approved Scanning Vendor - validate adherence by performing vulnerability scans of Internet facing environments of merchants and service providers

- **Section 6.6** focuses on securing Web applications. It has been in the standard as a best practice but will become a **requirement** effective **June 30, 2008**
- Requirement
 - Ensure that all Web-facing applications are protected against known attacks. This can be accomplished by:
 - Assessing your applications using one of the four options – Manual Review, Source Code Scanning tool, manual assessment (internal or third party), or Web application security vulnerability assessment tools
 - Using a Web Application Firewall (WAF) – Using a WAF however doesn't eliminate the need to do a secure software development process. In other words, you still need a vulnerability assessment so the vulnerabilities can be fixed to protect your data from hackers
- **Section 11.3.2** also further emphasizes the need for regular application-layer penetration tests to ensure that applications don't have vulnerabilities.

Penalties

- Visa may charge your business up to **\$500,000 per incident** if your network and the information of consumers is compromised
- Potential ban from use of credit cards
- Up to **\$100K per incident** for not notifying companies of any breach
- Acquirers whose Level 1 and Level 2 Merchants are not compliant will be fined between **\$5K and \$25K per month**
- Various other fines may also be imposed



- Level 1 merchants need a Qualified Security Assessor (QSA) to complete the Report on Compliance and present the report to the merchant/service provider's acquirer. MasterCard also allows an auditor to file this report instead of a QSA.
- For Level 2, 3 (and sometimes 4) merchants and service providers, responding to the PCI Self Questionnaire a must.
- PCI Self-Questionnaire is a check-list that requires them to certify that they have gone through and met all the twelve requirements including a scan from a PCI-ASV
- The questionnaire needs to be sent to your acquiring Bank
- Even one “No” on the questionnaire will make the merchant non-compliant with PCI
- Requirements are a little less stringent for Service Providers

Is PCI Compliance Enough?



- **No.**
- Although an important step, companies need to think about securing the Web applications and not just a checkbox
- Vulnerabilities provided in Section 6.5 as a guideline for testing are good but it's not a comprehensive list
- There are a lot more vulnerabilities in Web applications that hackers can attack through like session hijacking, privilege escalation and many others
- Many ASVs are not doing an in-depth testing of your applications. They'll get you certified but leave your applications insecure.

- PCI Standard Version 1.2 will be released in October, 2008
- No additional requirements are expected
- Existing twelve sections will be clarified
- There will be a lot more emphasis on securing Web applications not just the network
- Hackers will continue to attack through the Web application layer due to many vulnerabilities



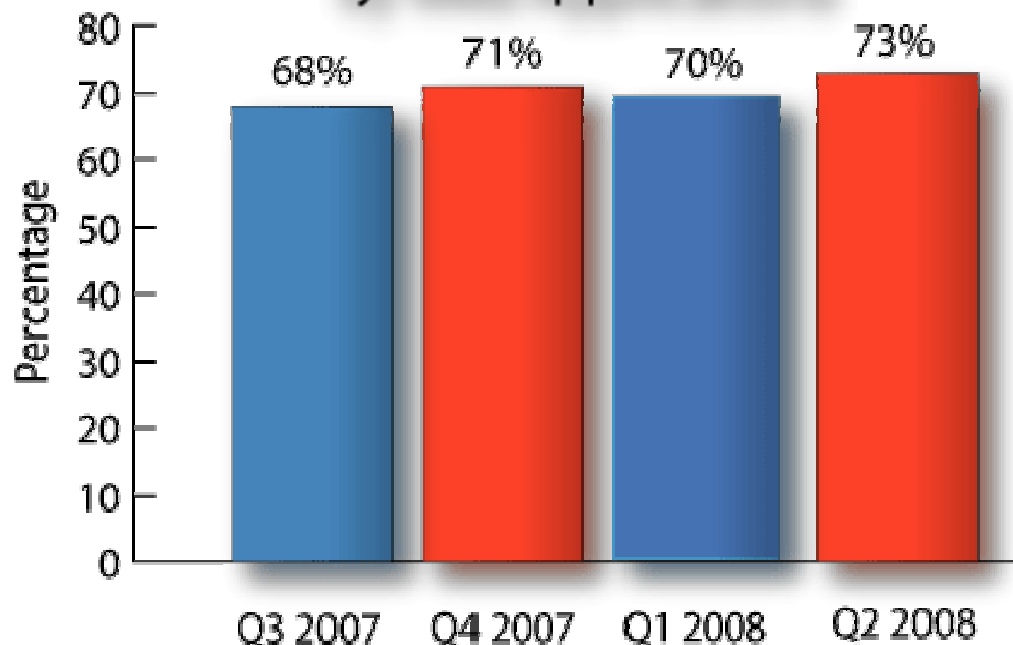
- "75% of cyber attacks & Internet security violations are generated through Internet Applications"
Source: Gartner Group
- 7,236 vulnerabilities reported in 2007; up from 5,990 in 2005
Source: CERT
- *58% of total vulnerabilities are Web vulnerabilities*
Source: Symantec Threat Report – 2008
- 73% of easily exploitable vulnerabilities affected Web applications
Source: Symantec Threat Report – 2008

400+ New Vulnerabilities a Month and Growing

Cenzic Q2 2008 Web Security Trends Report



Percentage of Total Vulnerabilities Comprised
By Web Applications



Software

Hailstorm® Enterprise ARC™

Flagship product for securing applications, accessible over the Web and used by the entire organization.

Hailstorm® Professional

Desktop software product for Web application security testing.

SaaS

ClickToSecure® ARC™

Remote assessment of Web applications using Hailstorm technology combined with human security expertise. No software to install. No installation required.

Professional Services

Assessment Methodology

Get a thorough assessment of your Web vulnerabilities in just 3 days from Cenzic's security experts team.

Training

Product & application security training including best practices.

Hybrid

Hybrid Model

Combination of both software and SaaS offerings, allowing you to do your own vulnerability assessments (using software) as well as receiving remote assessments from Cenzic (SaaS offering) when personnel and/or skill-set is lacking.

Beyond PCI Compliance

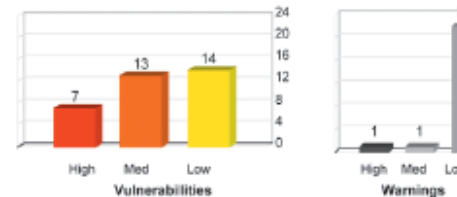


- Cenzic ClickToSecure[®] ARC[™] is PCI Compliant
- Using Web application best practices will ensure compliance with a variety of regulations including PCI
- June 20, 2008 = next PCI deadline
- Inquire about Cenzic's SaaS offering to provide a quick and easy way to become compliant



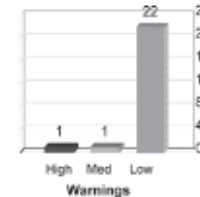
The 'Total HARM Score', above, is a sum of the HARM scores for all the SmartAttack assessments included in this report. SmartAttacks have different HARM scores based on the risks associated with each kind of vulnerability. The charts reflect the raw HARM scores without application specific risk adjustments.

Severity of PCI Findings



Severity Drill Down

Severity Drill-down w/info Items



Pages Tested	40
Attack Count	108276
Informational Items	105

Note: High, Med, & Low relate to the severity of the findings. Warnings are findings for which there is less confidence of accuracy. These items may or may not be real vulnerabilities.

SmartAttack	High Severity		Medium and Low Severity	
	Vuln.	Wam.	Vuln.	Wam.
Non-SSL Password	4	0	7	0
Cross-Site Scripting	3	0	4	0
Buffer Overflow	0	1	1	0
Directory Browsing			0	1
File & Directory Discovery			0	22
SQL Error Message			1	0
Check HTTP Methods			14	0
Web Server Version Vulnerabilities				
HTML & JavaScript Comments				

April/May 2008 Cenizic Accolades from Independent Publications



Winner:
Cenizic Hailstorm
Enterprise ARC 5.5



Winner:
Cenizic

Product Rating

Features	★★★★★
Ease of Use	★★★★★
Performance	★★★★☆
Documentation	★★★★☆
Support	★★★★★
Value for Money	★★★★★
Overall Rating	★★★★★



For: Integration with VMware is a unique and useful feature.

Against: None that we found.

Verdict: True enterprise-class product with impressive options and customizations. SC Magazine recognizes the Cenizic Hailstorm Enterprise ARC 5.5 as this group's Best Buy.



2 Awards Winner: Cenizic

1. Best Vulnerability Assessment Solution for the Enterprise
2. Best Security Testing Solution for the Enterprise

Cenizic Bags a Spot In "RED HERRING 100 NORTH AMERICA"

Winner: Cenizic



Cenizic Named CODiE Award Finalist for "Best Data Security Solution"



Questions?

Mandeep Khera, VP of Marketing

www.cenzic.com / *1-866-4-CENZIC (1-866-423-6942)*