NEbraska CERT Conference 2007

Computer Security and Information Assurance

Not sanctioned by :

PCI Security Standards Council™

# Data Security Standard 1.1 – Current Developments

**Michael Hoesing CISSP, CISA, CCP, CIA, CPA**

**m-hoesing@cox.net (an individual citizen)**

Positions presented herein are the opinions of the presenter formulated across various clients, industries and years of experience. Any applicability to your environment will be determined by your testing and your other due diligence. The presenter, their employers and conference sponsors accept no liability for any of this content applied in your environment.

# Agend a

History (VISA, 1999, 2003 , 2006, 2007 breaches, get tough, then CAP, fines, shift liability) (3)

The PCI/DSS Standard 1.1 (Map to ISO 17799) (4-5)

PCI Council (new director, call for input, board of advisors, Sept meeting) (6)

Assessors (scan methodology, qualification, independence, licensed?) (7)

Assessments & Associations (sampling?, other evidence gathering standards) (8 - 10)

LAWs (Minn, Federal - will FTC take over?) 11

Nuances remote access, app firewall, defense in depth, compensating controls, Map PCI/DSS to VMware ESX 12-16

Resources (17)

Drill Down – map PCI to VMware ESX 3.0.1 (18- 30)

# Histor
# y

**Each Association had a program and standards and security requirements (VISA CISP 1999 education focus & MasterCard SDP, Discover, AmEx,…, 2001 VISA we really mean it)**

**2003 Acxiom breach, Beltway Conversation with VISA?, suddenly the 1999 program became a requirement**

**2004 Choicepoint (front door, non-technical)**

**2005 Card Systems Solutions, public hearings,  CSS was PCI certified, every state attorney general filed a lawsuit, CSS out of business, acquiring bank sponsor experienced pain also**

**2005 VISA-Shaunessy carrot , train assessors, qualify assessors**

**2005-2006 more Internal and External Breaches, Identity Theft epidemic**

**Sept 2006 PCI Council formed and modifies the DSS 1.1**

- PCI DSS 0.0 Aug 2003    ,    PCI DSS 1.0 Dec 2004

**2006 TJX 40 mil cards, prolonged breach, PCI certified**

# PCI Mapped to Other Standards

| ISO 17799 June 2005 | NIST 800-53 | PCI DSS | COBIT 4.1 | ISACA |
|---|---|---|---|---|
| 4. Risk Assessment | RA 1-5 | 12.1.2 | P 09 | G 13, P1, P5 |
| 5. Security Policy & Training (8.2) | PL 1-5<br>AT 1-4 | 12<br>12.6 | DS 05, 07<br>P 06 | |
| 6. Organization of Information Security | | | P 04 | |
| 7. Asset Management | AC 15-16 | 3 | P02,05,10 | |
| 8. Human Resources Security | PS 1-8 | 12.7 | P 07 | |
| 9. Physical & Environmental Security | PE 1-17 | 9 | DS 12 | |
| 10. Communications and Operations Management, Media Handling including 3rd Parties (6.2)and Monitoring and Assessment (15.3) | AC 17-20<br>SC 1-19<br>CM 1-7<br>MP 1-6<br>SA 9<br>SA 1-12<br>CA 1-7 | 1, 4<br>5 (AV)<br>9.5-10<br>12.8<br>6 (vul)<br>11 | DS 01, 05<br>DS 06<br>DS 13<br>DS 11<br>DS 02<br>ME 01<br>ME 02 | G24,25,<br>P6<br>P 4<br>G 16<br>P 3<br>P 8 |

# PCI Mapped to Other Standards - 2

| ISO 17799 June 2005 | NIST | PCI | COBIT | ISACA |
|---|---|---|---|---|
| | 800-53 | DSS | 4.1 | |
| 11. Access Control | AC 1-14<br>AI 1-7 | 2, 7, 8 | DS 05 | P 2 |
| 12. Systems Acquisition, Dev & Maint (cryptography) Change Mgmt | SA 1-8, 10, 11 | 6<br>3, 4 | AI 1-7<br>PS 09 | G 14,23,29<br>P 9 |
| 13. Incident Management & Logging (10.10) | IR 1-7<br>AU 1-10 | 12.9<br>10 | DS 08<br>DS 10 | |
| 14. Business Continuity | CP 1-10 | 12.9 | DS 04 | G 32 |
| 15. Compliance | CA 6 (accredit) | | ME 03 | P 7 |

# PCI Council

## 2007 PCI council

- New director (Bob Russo), with a security background
- $2,000 membership and a voice
- May Call for input on “Navigating” document
  - 4.2 prohibits internal emailing of cardholder data
- Sept meeting Toronto
- 21 member board of advisors (financial inst & merchants)

## 2007 Small Company PCI/DSS “lite” debate (PCIco says no)

# PCI Assessors

**QSA and ASV , a filer can use different firms**

**$10,000, training, pass test (what is the pass rate?)**

**Independence not required, same security firm can sell & install devices, consult and perform assessment**

**Can not become ASV without PCI experience (CISSP value?)**

- (should security professionals be licensed? Like CPA’s?)

**Have Any Assessors been dis-barred, why? (Attorney or CPA license revocations and disciplinary actions are public)**

**CPA Financials are not taken at face value why are PCI assessments?**

# PCI Assessments

**Scanning –usually a proprietary (Nessus) process, comparable across assessors?**

**While the PCI/DSS ROC from VISA does include specific test procedures, there is no sampling standard as to which systems/devices/datastores will be reviewed**

**There is no periodicty standard – the tests can be performed in January for a December filing, test early remediate (if necessary), retest**

**All locations where credit card data exists, no materiality specified once you are in level one (visit a call center even if it has one person)**

# Association Programs

**VISA CISP**

- Levels, Merchants & Service Providers - 6 mil, 1 mil

**VISA CAP**

- Pay the Acquirers for successful PCI <u>FILINGS </u>by a<u> </u>QSA?
  - Carrot - 3/31/2007 Larger $$$ 8/31/2007 Not As Large $$
  - Stick – 10/1/2007 less favorable interchange rates

**(VISA) 2007 CAP evolution from funding to fines <u>on acquirer</u>**

> Having a Breach and Being Non-Compliant - $500,000
> Failure to Notify of Breach - $100,000
> Failure to be Compliant – $5 -25,000 / month per merchant
> Retaining Prohibited Data (16 digit, CVV, PVV, magtracks) - $10,000 / month per merchant

# Association Programs - 2

**Flip-Flops**

- “that’s the assessor’s call” – “that is up to the association to accept the filing”
- Regarding encryption3.4 and AV 5.1` “____X is a ‘proprietary’ operating system” “____X is not a proprietary operating system”

**Verified by VISA** [anyone using that?]

# Laws

Minnesota PCI Law – pay card issuers, specific damages

Notification of Risk to Personal Data Act (S 239)

- National Breach Law, recently re-introduced by Diane Feinstein:
- Would also require notifying the Secret Service if over 10,000 records were stolen, bureaus if over 5,000
- $1,000 per day PER CONSUMER ($1 mil cap)

Personal Data Privacy Act and The Cybersecurity Enhancement and Consumer Data Protection Act (S 495)

- Severe daily penalties and potential jail time for failure to report breaches, and for the unuathorized access (hacker fine)
- establish and implement data privacy and security programs
- Data brokers regulated by the FTC (pre-empts states)

# Nuance
# s

**The DSS is comprehensive, it is difficult to come up with a compensating control that is not one of the other DSS requirements, lack of credit for defence-in-depth**

- Networks – only a single tier is required by DSS
- Organization – independent CISO is not required

→ **The narratives in front of sections may govern the application of the succeeding standard section:**

- Section 3 – compensating controls can avoid encryption
- Section 6 – 30 day patch rule is out, testing & relevance govern

**SAPr Test Procedures may re-write the standard 8.5.9, 8.5.10,**

**Definitions – periodically 1.1.8, email 3 intro & 4.2**

**Interpretation & Negotiation may save (cost) significant $$$**

# Nuances – 2 Compensating Controls

**Compensating controls to avoid encryption if cardholder date in section 3.4 must meet ALL of the following:**

1. Document a risk assessment and business reasons for not encrypting
2. Must be controls not required in other sections of the PCI/DSS
3. Provide additional segmentation (usually at the network layer)
4. Provide access restrictions based on
    - □ IP or MAC address
    - □ Application or Service
    - □ User Accounts or Groups
    - □ Packet Filtering
5. Access control outside of Active Directory or LDAP
6. Prevent/Detect application or database attacks (i.e. SQL injection)

# Nuances - 3

- 3.6.4 Annual encryption Key changes (for PINs ??)
- 6.6 New Section on Web Applications
  - What is the definition of a web application firewall? (rqd 6/08)
  - A web app firewall is equal to an app that passes an OWASP assessment?
  - Can internal staff scan web applications?
  - Frequency of web app scans not defined
- 8.3 Remote access to card data requires 2 factor authentication by employees, administrators and third parties (but not for 300 million cardholders)

**SAPR 8.5.9, waiving the 90 day password change rule for service provider supplied software to merchants; conflicts with PABP 3.1 (Payment Application Best Practices) 90 days regardless**

**9.7.1 – Data Classification is Required (not just labling)**

# Nuances - 4

**11.1 Quarterly Wireless Scans (prove something doesn’t exist ??)**

**11.3 Pen Tests must include both network pen and application pen (which apps??)**

**11.5 File Integrity Monitoring went from daily to weekly??**

**12.6.1 Employee Info sec Training – at hire and annually**

**12.8 Service Provider Contract items no longer needed:**

- BCP terms
- Audit terms
- Termination Requirements

# Nuances - 5

“Agents” – they don’t process, store, or transmit, but they still must be PCI compliant if ‘accessing’ 16 digit card number (call center vendor with remote access) (define ‘transmit”)

One DSS – applied equally to acquirers and issuers and their service providers?

“Transactions” – originally web based only

Original DSS - processors had to physically segregate data?

Whole new appendix A for hosting business

# Resources

https://www.pcisecuritystandards.org/

http://pcifile.org/phpBB2/index.php

http://www.pcicomplianceguide.org/step2f.html

http://pcianswers.com/

http://usa.visa.com/merchants/risk_management/cisp.html

http://securitybuddha.com/2007/03/23/the-problems-with-the-pc
/

NEbraska CERT Conference 2007
Computer Security and Information Assurance

Not sanctioned by :

PCi Security Standards Council ™

# Data Security Standard 1.1 – Applied to VMware ESX 3.0.1

**Michael Hoesing CISSP, CISA, CCP, CIA, CPA**
**m-hoesing@cox.net**

Positions presented herein are the opinions of the presenter formulated across multiple clients, industries and years of experience. Any applicability to your environment will be determined by your testing and your other due diligence. The presenter, their employers and conference sponsors accept no liability for any of this content applied in your environment.

# The VMWare ESX - PCI Big Three

## Hot Spots:

- Protect Root access on ESX host COS/VMkernel
  - Strong password, SUDO
- Protect Remote Access
  - High remote setting (default), root SSH disabled (default)
- No Tiered Networks
  - All VMs connected to one vswitch (realistic? Conflict with other security configurations [i.e. segregate Dev & Prod, or BlueLane]?)
  - Not an automatic failure, assessor education needed, compensating controls, defense in depth, greater good,

# PCI Compliance Mapped to VMware VI Environment

## 1.x Firewalls:

- Iptables built-in to ESX 3 , have a policy/build standard
- Ports open should only be VMware supported and documented exceptions (443,902 903,2049 3260 8000, 27000 27010, 5988 5989, 2050 thru 5000, 8042 thru 8045)
- Understand vswitches and what is running on each (production, management, iSCSI, VMotion, )

## Assessment:

- Ecora baseline report enumerates ports
- Console commands = Iptables –l   route   nmap from a remote
- Virtual Center = host, configuration tab, networking

# PCI Compliance Mapped to VMware VI Environment

## 2.x Configuration:

- document a policy or a build standard
- No other applications on the ESX host
- Stay current on VMware patches
- Encrypted remote admin sessions
- Remove/change vendor defaults (snmp public?)

# PCI Compliance Mapped to VMware VI Environment

## 2.x Assessment:

- Ecora baseline report enumerates many configuration settings and devices, security configs, change reports show drift (if any)
- Console commands - esx-info, rpm –qa, lspci, ps aux, lsmod, cat /vmfs/volumues/vmname/guestname.vmx
- Other tools - LSAT will compile "make" is installed, Bastille –assess, MTH script
- rpm –qa --changelog | grep CVE (shows what vuls are patched)
- cat /etc/ssh/sshd_config , host-> Config -> Security Profile
- cat /etc/snmp/snmpd.conf (make sure "Public" is not present)

# PCI Compliance Mapped to VMware VI Environment

## 3.x Data Encryption at Rest:

- Secure the SSH & SSL keys (CVE 2006-2481 for ESX 2.x)
- No data stored on ESX host

## Assessment:

- Ecora will cite SSH and SSL version numbers
- Ls –l /ets/ssh/ and /etc/vmware/ssl , user and group permissions should be only root (see VMworld lab to protect SSL key)
- Difficult to prove what shouldn't be there, is not there:
  ls –l /tmp    or    find / -mtime n (days since install date)
  ls –l /var/core   ls –l /var/log/messages | grep <searchterm>

# PCI Compliance Mapped to VMware VI Environment

## 4.x Encryption Data in Transit:

- Use SSH & SSL

## Assessment:

- Ecora will cite SSH and SSL version numbers
- cat /etc/ssh/ssh_config   for strong algorithm
- cat /usr/share/ssl/opensll.cnf
- cat /etc/vmware/hostd/config.xml

## 5.X Anti-Virus

- Assuming ESX is “UNIX-based” , it is exempt
- recommended in Server Configuration Guide

# PCI Compliance Mapped to VMware VI Environment

## 6.x Vendor Patches:

- Check the VMware knowledgebase for the latest
- Don’t mix Dev and Prod VMs on the same host
- Was web access to the COS UI developed under OWASP?

## Assessment:

- Ecora will cite kernel version numbers
- Analyze rpm –qa --changelog output, match to CC docs
- Analyze  rpm –qa for internally developed software
- Review Virtual Console network diagrams and maps
- Run Webinspect against the httpd/Tomcat features on the host

# PCI Compliance Mapped to VMware VI Environment

## 7.x User Access:

- Limit Administrators or other powerful users to their job functions
- Don’t mix Dev and Prod VMs on the same host

## Assessment:

- Ecora will cite list users and groups and permission roles, compare these to their job functions
- Review sudo users on the host    cat /etc/sudoers

# PCI Compliance Mapped to VMware VI Environment

**8.x IDs and Passwords:**

- No duplicate ID’s
- 2 factor remote network access
- Encrypt passwords
- Password metrics

**Assessment:**

- Review  /etc/shadow for duplicates
- Review location of ESX hosts in the network and their access
- Review that all accounts are in /etc/shadow /etc/security/opasswd
- /etc/login.defs or PAM config for 90, 7, AN, **4**, 6

# PCI Compliance Mapped to VMware VI Environment

## 10.x Track and Monitor:

- Associate administrative access to individuals
- Log system activities & events
- Synchronize clocks

## Assessment:

- Review sudoers
- Ensure 5 log files are being created, secured and reviewed
- Review log records /varlog/vmksummary and others for user, date/time, event, origination
- Review syslog.conf for log centralization
- NTP recommended review ntp.config

# PCI Compliance Mapped to VMware VI Environment

## 9.x Physical Security:

- Nothing unique to VMware, however  make sure everywhere you VMotion, copy, backup an in-scope VM has the same physical security as production

## 11.x Regularly Test

- CMDB validation, vul scans and pen tests should cover hosts
- Network IDS/IPS should cover host traffic
- File integrity monitoring (Tripwire  sha1sum) at least on logs 10.5.5

## 12.X Policy:

- Or a build/configuration standard not only covering the host configuration but also attached components (Ecora or lspci or , deployment strategy (tiers, dev, prod, storage, backups)
- InfoSec involvement (certification, permission granting)

# Ten Ways to Create a Sustainable IT Compliance Program

1. Automate
2. Evaluate and adjust
3. Self-assess
4. View compliance as an opportunity
5. Be practical
6. Understand financial flows and business effect
7. Manage your controls
8. Leverage tools with other benefits
9. Use metrics to test controls
10. Don’t reinvent the wheel

*IT Compliance For Dummies, Limited Edition*
Wiley Publishing, Inc.