GTC

PCI – DSS
Payment Card Industry
Digital Security Standard

Ira Victor, GIAC G17799 GPCI GSEC
Director, Compliance Practice

Agenda

1. Acknowledgements
2. History of The Standard
3. Overview of *The Digital Dozen*
4. Links

Acknowledgements

Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com

1. PCI Security Standards Council: Created the Standard, quoted in the titles, and other content for this presentation

2. SANS Institute: Best source of real-world PCI information, and best training for PCI Internal Auditor Certification

3. InfraGard: Dissemination of cyber-crime information

PCI History

Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com

Initially:

VISA Standard

Also called the “Digital Dozen”

MasterCard Standard was close, but different

NOW:
Payment Card Industry Digital Security Standard
-Visa, MasterCard, Amex, Disco

Who Needs To Follow PCI?

Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com

-> All entities that process, store or transmit credit card data

Merchant Levels

Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com

-> **Level 1**

1. 6,000,000+ credit card transactions per year OR
2. Merchant has had a breach OR
3. Visa/MC/AMEX/Disco declares you as Level 1

-> **Level 2**

150,000 to 6,000,000 eCommerce transactions per year

-> **Level 3**

20,000 to 150,000 eCommerce transactions per year

-> **Level 4**

Less than 20,000 eCommerce transactions per year OR

Up to 6,000,000 non eCommerce transactions per year

Compliance for Merchants

Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com

-> **Level 1**

Once per year: on-site audit by an approved auditor, OR
On-site audit by an auditor and signed-off by corporate officer
Quarterly network scan by independent entity

-> **Level 2 & 3**

Once per year: Self-evaluation
Quarterly network scan by independent entity

-> **Level 4**

Recommended: Self-evaluation and network scan

Section 1 – "Build and Maintain a Secure Network"

Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com

Proper Firewall Configurations

1. Firewall Placement
2. Network Diagram
3. Network Management Roles
4. Required Services Only
5. Documented Change Control System

Section 1 – Allowed Protocols

Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com

Only the Following Are Allowed *

1. HTTP: Port 80, TCP
2. SSH: Port 22, TCP
3. SSL: Port 443, TCP
4. VPN: According to vendor spec

*Additional ports CAN be added but:

- MUST document the business need
- MUST have mitigating security elements
- MUST be properly secured

Section 1 – Secure Network

Proper Firewall Configurations

Must use “Deny by Default” principal

Any service that is NOT needed in the network

“Segregation of Services”

- Databases in DMZ?
- Desktop firewalls?
- Well managed routers?
- Control connections between card data and non-card data?

Control outbound connections: Egress Filtering

Stateful Packet Inspection – only pass stateful connections

Section 1 No Direct Public Access, NAT is REQURED

Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com

->No direct public access to CC data

Must implement complete mediation

What the heck is complete mediation?

- Mechanisms that erect total barriers and security checks between identified targets and anyone who tries to access them

Take away: properly configured firewalls, and disable all other access

->NAT/IP Masquerading/Network Masking is required

- The source and/or destination addresses of IP packets must be rewritten as they pass through a router or firewall

Section 2 – "Do Not Use Vendor-Supplied Default Passwords and Other Security Parameters"

Must change the Default Settings for all systems used to support, contain or transmit CC information

This includes non-obvious systems like: printers, VPN concentrators, VoIP systems, Wireless systems and all other systems

Wireless should not be used, if it is: MUST disable wireless administrative access, MUST encrypt data, MUST turn off SSID

Section 2 – Standards for Configurations, and Administrating Systems

Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com

Organization must develop written configuration and deployment standards

- One major function per server
- Only run necessary services
- ID and configure security needs to the specifics of that system
- Remove all unnecessary services, drivers, features, etc

Administrating Systems

- ALL remote connection access must be encrypted
- Disable non-encrypted console access
- Wireless devices must only allow admin access from the wired network and MUST be encrypted

Section 3 – “Protect Stored Data”

Must document legal, regulatory, and business requirements

Must document disposal

Must document offsite and other transfer procedures

Is your organization….

- Encrypting confidential data, including backup?
- Storing and protecting un-needed data?
- Implementing a data lifecycle plan?
- Storing important logging information?

Section 3 – What NOT to Store

Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com

-> Don't ever store the card verification number
  - *Non-embossed* number *printed* on the card
  - VISA: "C V V 2" (Card Verification Value)
  - MasterCard: "C V C 2" (Card Validation Code)
  - AMEX/DISCO: "C I D" (Cardmember ID)

-> Don't ever store the PIN number

-> Don't ever store the magnetic strip data

-> Check databases for info in another field

Section 3 – Masking

Masking portions of the credit card and other data

Workers should only be able to view a portion of the confidential data

Standard mandates that only the smallest amount of data be viewable as needed by the business

But…one of the the most important part of masking….

Section 3– Masking (con't)

Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com

** Can only show the last four digits OR last six digits. This includes transaction receipts

NO BRAINER: Add this practice to web and non web privacy policies

Berkeley Flower Power Shop
Main ST
Berkeley, CA 94704

Date: Dec04'04 04:47PM

Egyption Goddess Patchouli	595.00
7.00 x 85	
Henna Tattoos	728.00
14.00 x 52	
Family First: Dr. Phil McGraw	26.00
26.00 x 1	
Cauldron, etched Pentacle	350.00
350.00 x 1	
Druid Mask	135.00
DISCOUNT 10%	
Cards, Thank you	5940.00
.99 x 6000	
SUB TOTAL	7774.00
SALES TAX	621.92
TOTAL	8395.92

AMOUNT TENDERED
Card Type: SPIRIT OF AMERICA VISA
Acct #: 131

TOTAL PAYMENT 8395.92

Hugh Hewitt

Thank you for shopping at
Berkeley Flower Power Shop!
Peace Out!

Section 3 – More on Stored Information

All stored confidential must be encrypted, truncated or hashed

Databases, of course

** Also Important, Protection For**
Removable media and logs that contain confidential information

Proper protection regarding removable media and logging very often over-looked

Section 3 – Hashes and Crypto

Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com

All stored confidential must be encrypted, truncated or hashed

What is a “Hash?”

A process that takes data of any length, and produces a result of one length.

The process is not reversible

But, CAN be duplicated and used to compare

Encrypted – the original contents are “jiberish”

AES-256 and 3DES

Section 3 –Stored Information (con't)

Credit Card Data

Databases, of course

** Also Important, Protection For**
Removable media and logs that contain confidential information

Proper protection regarding removable media and logging very often over-looked

The keys used in encryption must be properly managed

Open Source StrongAuth.com is worth a look

Section 3 –Must Not Disclose Keys

-> Limit the number of people with access to crypto keys

-> Protect systems that manage the crypto keys

Open Source StrongAuth.com is worth considering to manage this important issue, too

Section 3 –More Managing Crypto Keys

Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com

Must manage the entire process of Crypto Key Management

- Creating the encrypted keys
- Securing the distribution of the encrypted keys
- Keeping the stored encrypted keys safe
- Creating procedures for revoking, changing and destruction of encrypted keys
- Incident response in case of compromise of encrypted keys

Section 4– “Encrypt Transmissions of Cardholder and Sensitive Information Across Public Networks”

Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com

->eCommerce

- Secure Socket Layer - SSL
- 128-bit encryption
- Certificates must be valid

->eMail of confidential information must be secured

Nothing specific in the standard, GPG and TrueCrypt are open source products to look into

Section 5 – “Use and Regularly Update AV software or programs”

Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com

- Anti-Virus Best Practices
- Covers both desktops and servers
- Layer of anti-virus
- Up-to-date patterns
- Periodic scans
- Suggested: Layers and good logging, can make a difference in protecting data

Section 6- “Develop and Maintain Secure Systems and Applications”

-> Written policies in place, as part of change control written policies

-> Test patches with small sub-set of systems, or testing systems

-> Must apply patches within 30days of release

Section 6 - Application Development

6.3 is most concerned with best practices in application development

- Security planned from the beginning, not adding security as a "check off"
- Software creation and security are kept separate, "Separation of Duties" are really important
- Why can't software developers cannot effectively test and audit their own team's code?
- Code and code changes must be reviewed under the same standard
- Best practices in web app development. Examples: Cross site scripting, buffer overflows, data validation, session controls, errors, DOS, access controls, and others

Section 6 Vulnerability Assessment

-> Not network scanning (that's elsewhere)

-> Strategic approach to vulnerability assessment

-> Alert services, SANS, FBI Alerts through InfraGard. Must keep current on threats and countermeasures, and document it!

Section 6 - Change Control

Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com

- Must put into practice written change controls
- Impact Analyses: why is the change needed
- Approvals: who signed off on the changes?
- Testing Procedures: the types of tests run and the results
- Unwind Procedures: procedures if the changes have to be undone

Section 7 – "Restrict Access to Data by Business Need-to-Know"

Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com

Data access must be controlled using "Least Privilege"

From NIST:

"The principle of least privilege requires that a user be given no more privilege than necessary to perform a job."

"Ensuring least privilege requires identifying what the user's job is, determining the minimum set of privileges required to perform that job, and restricting the user to a domain with those privileges and nothing more."

-> Documentation needs to describe how you have implemented Least Privilege

->Don't forget your *audit trails*!

Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com

Even AFTER authentication must still apply:

1. Access measures with the applications
2. Deny all unless user has specific permissions
3. Allowed access based upon need only
4. Allowed access by documented job description

Section 8 – "Assign a Unique ID to Each Person with Computer Access"

Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com

ALL users must have unique IDs that are logged and managed

Authentication can be by:

1. Password/Passphrase
2. Biometrics
3. SecureID-type tokens
4. Smart Cards
5. Digital Certs

Must use TWO FACTORS for remote access

Credentials: hashed or encrypted in transit and/or at rest

Section 8 – More on IDs

Organization must have a formal ID management policy

That policy needs to include:

1. Who is allowed to have access and what level of access
2. Password creation, reset, revocation, and removal policy
3. Creation of unique first time passwords
4. Disable all vendor default accounts, “back doors”
5. Lock out console access

Passwords changes every 90days or less
7+ characters in length, numbers and letters
History: 4x, Lockout:6x and 30min; No use timeout: 30min
SQL queries and database access is restricted

Don’t forget: *audit trails!*

Section 9 – "Restrict Physical Access to Cardholder Data"

Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com

Gates, Guards and Guns

1. STRONG locks
2. Surveillance Cameras
3. Control RJ14 jacks and network gear
4. Badge controls
   - Visitors must be escorted
   - Visitors must wear badges
   - Visitors cannot go to areas with confidential data
   - Visitor badges must be easily IDd
   - Extensive logging info on visitors, keep for at least 90days
   - Badge control upon exit

->Don't forget your *audit trails*!

Section 9 – BackUps!

Goal: Cannot access the confidential information

1. Off-site, secure and provisions for fires
2. Encrypted in transit and at rest
3. Paper backups must be secured, too
4. Cross-cut shred of paper waste
5. Properly managed/"labeled" for accurate accounting
6. Proper electronic shredding, or destruction

->Don't forget your audit trails!

Section 10 – "Track and Monitor All Access to Network Resources and Cardholder Data"

Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com

….Being able to prove it!
Must have logging turned on and properly stored

Track all activities and access of confidential information
Track all administrative activities, including logging information
Track failed access attempts
Track access to ID system
Track all begin/end/deletes on logs
Track creation and deletion of system level objects

Checks alerts and issues daily

-> Documentation the policy

-> Logging applications can help manage with process

Section 10 – Time and Logging Lords

Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com

- Must have TWO internal clock servers syched with NTP (or similar)
- Internal servers must not look to external time servers
- Must re-set MSFT default settings
- Logging systems need to secured against unauthorized changes
- Logging systems records need to be backed up to a secure central system
- Logs should be hashed to ID changes
- Logs available online for 90days, on tape or online for 365 days
- BETTER: Non-reputable logging system

Section 11– "Regularly Test and Security Systems and Process"

Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com

Put into place protective controls, detective controls and reactive controls

Protective Controls: Preventative measures taken to mitigate a risk of
Example: Firewalls, access controls

Detective Controls: Detect errors and abnormalities
Example: IDS systems, audit trails

Reactive Controls: Respond when a issue is detected
Example: IPS systems, incident response procedures

Section 11– Vulnerability Scans + Pen Test

External Scans by an approved vendor

Good idea to have an internal scanning team on an on-going basis

Qualys, CoreSecure, Nessus are all quality solutions

Penetration Test: Ethical Hacking to get access to confidential data

ALSO in Section 11

- Intrusion Detection
  -> Tie IDS into logging system
- Monitor File Integrity
  -> Web server, applications, etc.

Section 12 – "Maintain a Policy That Addresses Information Security for Employee and Contractors"

Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com

Ten Mandated Policies (*quoted from the PCI Standard #12*)

1. Explicit management approval
2. Authentication for use of technology
3. A list of all devices and staff with access to those devices
4. Labeling of devices with owner, contact info and purpose
5. Acceptable used of the technology
6. Acceptable network locations for these technologies
7. A list of company approved products
8. Auto disconnect of modem sessions after a specific period of inactivity
9. Activation of modems for vendors only when needed by vendor, with immediate deactivation after use
10. When accessing cardholder data remotely via modem, disable storage of cardholder data onto local hard drives, floppy drives or other external media. Also disable cut-and-paste, and print functions during remote access."

Section 12 – More on Policies

Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com

- Policies must be written down and conform with the PCI standard
- Must also include risk assessments
- Regular (annual), formal review
- Can't collect dust – must have training and dissemination of policy to staff, partners, suppliers, consultants
- Two policies: one for staff, the other for management
- Appoint a "security leader"
- Require vendors, partners and contractors to adhere to PCI
- Testing and incident response

Links

- PCI Council – pcisecuritycouncil.org
- SANS: sans.org
- InfraGard: Infragard.org
- StrongAuth: StrongAuth.com
- Nessus: Nessus.org

Re-Cap

Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com

1. Acknowledgements
2. History of The Standard
3. Overview of *The Digital Dozen*
4. Links

GTC

Security Beyond The Perimeter

Q&A

Ira Victor, GIAC G17799 GPCI GSEC
Director, Compliance Practice