20 Questions for your IT Department Including PCI
1. What standard do they use?

• A way to measure your security stance
• NIST, ISO, COBIT are examples
• Typical audit findings
  – No standard used
  – Not following industry best practices
• Why is it important?
  – How do you prove you are doing what you should be? (Due diligence)
  – Standards address common risks
  – Increase in performance
2. Do you have an Inventory?

- Hardware, Software and Licenses
- Best to have a continual update process
- Perform a full inventory and true up at least annually
- Let senior management know of the result
- Typical audit findings
  - Inventory out of date
  - No inventory at all
  - Inventory does not match actual assets
- Why is it important?
  - Fines related to licenses
  - Missing equipment
  - Out of sight, out of mind, open for attack
3. Does someone monitor audit logs?

• Audit logging is a detective control
• Monitoring audit logs is a preventative control
• Typical audit findings
  – Audit logs not turned on
  – If audit logs are turned on, they are not monitored
• Why is it important?
  – Accountability
  – Proactive approach
4. Do they control administrative privileges?

• Principle of least access
• Access only to what is needed
• Typical audit findings
  – Administrative passwords are not changed
  – Users are local administrators
  – IT department users use administrator/root

• Why is it important?
  – Administrative rights give attackers greater access to your systems
  – Increases the impact of an incident
5. Is access based on need to know?

• Related to #4
• Includes excessive access
• Typical audit findings
  – File shares with “everyone” access
  – More access than needed for job function
  – Data owners don’t know who has access to their data
• Why is it important?
  – Will limit the impact of incidents
  – Limit unnecessary disclosure
6. Does someone monitor account administration?

• Who watches the watchers?
• Often administrative accounts have access above all other accounts?
• Typical audit findings
  – Excessive administrative privilege use
  – No one knows what Administrators do to systems
• Why is it important?
  – The ability to find incidents during the normal course of business
7. Do you have malware defenses?

• Not just Anti-virus
• Malware, spyware, adware, virus, worms, pop-ups, Trojans
• Typical audit findings
  – Anti-virus not kept up-to-date
  – Not on all machines, typically the ones not on the inventory
  – Only anti-virus, not covering all malware
  – Virus activity reports are not shared with Management
• Why is it important?
  – Still a big problem
  – Downtime
  – Attackers use this as an attack vector still
8. Do you have data loss prevention?

• How do you stop data leakage

• Information floods out of organizations

• Typical audit findings
  – No idea what data loss prevention is
  – No data loss prevention strategy or data classification
  – Suffer from the illness that “everything” is public

• Why is it important?
  – Liability (PCI data, HR data, etc...) $$$
9. Do you have vulnerability assessments?
• What holes do you have in your network?
• Know your weaknesses
• Typical audit findings
  – No vulnerability scanning
  – Not following up with vulnerabilities
  – No internal scanning
• Why is it important?
  – Most attacks are against vulnerabilities that have patches or fixes
10. Are there limits set on your network?

- Limit access to network ports, protocols and services
- Only needed services and protocols should be allowed
- Typical audit findings
  - Access to network is not restricted
  - Unnecessary service and protocols
- Why is it important?
  - Attackers use these
  - More to manage, increased expenses
11. Do you have an incident response capability?

- Need guidelines on how to respond
- Include evidence preservation
- Typical audit findings
  - No incident response capability
  - No training, no idea what is needed
- Why is it important?
  - How an incident is handled will determine if you can take legal action, determine the extent of a breach, stop the incident
  - Liability $$$
12. Do you have data recovery capability?

• It is one thing to have backups, it is entirely different thing to recover
• Typical audit findings
  – Backups not tested
  – Backups onsite
  – No business continuity plan covering IT (EOC)
  – Data owners are not informed of the backup strategy or data retention
  – Backup media is not accounted for
• Why is it important?
  – How much downtime can you tolerate?
  – What if you had to input everything from scratch?
13. Do you have a IT risk management process?

- IT control selection should be based on risk
- Protects against excessive and inadequate controls
- Typical audit findings
  - No formal risk management process (ad-hoc)
  - Control selection not based on risk
  - Risk and controls are not documented or formally accepted by data/process owners
- Why is it important?
  - Don’t want to over spend on IT security
  - Don’t want to under spend on IT security
14. Do you have separation of duties?

• Separation of duties in IT tasks as well
• Not for all tasks, just critical
• Typical audit findings
  – No Separation of Duties (SOD)
  – No idea what duties to separate
  – IT Management doesn’t identify single source knowledge experts
• Why is this important?
  – Prevents or limits fraud
  – Especially on financial systems
15. How do you manage 3rd parties?

• Get it in writing
• Included notification, security requirements and audit
• Typical audit findings
  – No formal agreement
  – No monitoring of 3rd parties
  – No notification provision
  – No provision to address data ownership at contract termination
• Why is it important?
  – Your responsibility to protect your data
  – You can transfer authority not responsibility
  – If they have a breach with your data don’t you want to know ASAP?
16. Do you have awareness training?

• Initial upon hire, annual classes, regular reminders
• Including acceptable use (Internet/Email)
• Typical audit findings
  – No ongoing training
  – Ad hoc, no records for initial training

• Why is it important?
  – Continuous reminder
  – Just like safety awareness
17. What do you have for wireless security?

- Limit wireless access
- On a separate network
- Best available encryption
- Typical audit findings
  - No encryption or weak encryption (i.e. WEP)
  - Rouge access points
  - On internal network
  - No monitoring of activity
  - Data owners aren’t notified of the risk
- Why is it important?
  - It is the easiest way into your network
18. Do you have application security?

• Security has layers
• Don’t neglect application security
• Typical audit findings
  – Strong network controls weak ERP controls
  – Audit logs, access control, etc...
  – Data owners don’t know who has access to their data
• Why is it important?
  – If you have a control failure you can still stop an attack
  – Network controls focus on external threats not internal
  – Generally internal fraud will include application data
19. Do you manage mobile devices?

• Control what they connect to when not in your environment
• Laptops, phones, USB devices
• Encryption
• Typical audit findings
  – No control on what connects to your network
  – No protect if it is stolen
• Why is it important?
  – Theft
  – Data leakage
  – Bring malware into your environment
20. Are you PCI compliant?

• If you take credit cards in any way shape or form, you have to comply with the PCI Data Security Standard

• Typical audit findings
  – Finance thinks it is a IT issue
  – IT thinks it is a Finance issue
  – Not compliant

• Why is it important?
  – There is a reason for the controls
  – $$$ Liability
Maze & Associates Audit Findings

- 54 local governments, Cities, Districts, Agencies, JPAs
- NIST SP 800-53 rev2
- 210 controls in 17 families, based on a moderate risk system
- Standard maturity matrix (0-5)
- Risk level: Low, Moderate, High

<table>
<thead>
<tr>
<th>Section</th>
<th>Average Maturity</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACCESS CONTROL</td>
<td>2.60</td>
</tr>
<tr>
<td>AWARENESS AND TRAINING</td>
<td>1.74</td>
</tr>
<tr>
<td>AUDIT AND ACCOUNTABILITY</td>
<td>2.20</td>
</tr>
<tr>
<td>CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENTS</td>
<td>2.14</td>
</tr>
<tr>
<td>CONFIGURATION MANAGEMENT</td>
<td>2.44</td>
</tr>
<tr>
<td>CONTINGENCY PLANNING</td>
<td>2.05</td>
</tr>
<tr>
<td>IDENTIFICATION AND AUTHENTICATION</td>
<td>2.54</td>
</tr>
<tr>
<td>INCIDENT RESPONSE</td>
<td>1.60</td>
</tr>
<tr>
<td>MAINTENANCE</td>
<td>2.55</td>
</tr>
<tr>
<td>MEDIA PROTECTION</td>
<td>2.59</td>
</tr>
<tr>
<td>PHYSICAL AND ENVIRONMENTAL PROTECTION</td>
<td>2.56</td>
</tr>
<tr>
<td>PLANNING</td>
<td>1.88</td>
</tr>
<tr>
<td>PERSONNEL SECURITY</td>
<td>2.73</td>
</tr>
<tr>
<td>RISK ASSESSMENT</td>
<td>1.78</td>
</tr>
<tr>
<td>SYSTEM AND SERVICES ACQUISITION</td>
<td>2.67</td>
</tr>
<tr>
<td>SYSTEM AND COMMUNICATIONS PROTECTION</td>
<td>2.74</td>
</tr>
<tr>
<td>SYSTEM AND INFORMATION INTEGRITY</td>
<td>2.80</td>
</tr>
<tr>
<td>DOCUMENTATION</td>
<td>1.92</td>
</tr>
</tbody>
</table>
## CCC General Control Audit Insights

| No | Question/What is it?                              | NA | 43% | 7% | 18% | 4% | 4% | 4% | 7% | 7% | NA | 4% | NA |
|----|--------------------------------------------------|----|-----|----|-----|----|----|----|----|----|    |----|----|
| 1  | What standard do they use?                       |    |     |    |     |    |    |    |    |    |    |    |    |
| 2  | Do you have an Inventory?                        |    |     |    |     |    |    |    |    |    |    |    |    |
| 3  | Does someone monitor audit logs?                 |    |     |    |     |    |    |    |    |    |    |    |    |
| 4  | Do they control administrative privileges?       |    |     |    |     |    |    |    |    |    |    |    |    |
| 5  | Is access based on need to know?                 |    |     |    |     |    |    |    |    |    |    |    |    |
| 6  | Does someone monitor account administration?     |    |     |    |     |    |    |    |    |    |    |    |    |
| 7  | Do you have malware defenses?                    |    |     |    |     |    |    |    |    |    |    |    |    |
| 8  | Do you have data loss prevention?                |    |     |    |     |    |    |    |    |    |    |    |    |
| 9  | Do you have an vulnerability assessments?         |    |     |    |     |    |    |    |    |    |    |    |    |
| 10 | Are there limits set on your network?            |    |     |    |     |    |    |    |    |    |    |    |    |
| 11 | Do you have an incident response capability?     |    |     |    |     |    |    |    |    |    |    |    |    |
| 12 | Do you have data recovery capability?            |    |     |    |     |    |    |    |    |    |    |    |    |
| 13 | Do you have a IT risk management process?        |    |     |    |     |    |    |    |    |    |    |    |    |
| 14 | Do you separation of duties?                     |    |     |    |     |    |    |    |    |    |    |    |    |
| 15 | How do you manage 3rd parties?                   |    |     |    |     |    |    |    |    |    |    |    |    |
| 16 | Do you have awareness training?                  |    |     |    |     |    |    |    |    |    |    |    |    |
| 17 | What do you have for wireless security?          |    |     |    |     |    |    |    |    |    |    |    |    |
| 18 | Do you have application security?                |    |     |    |     |    |    |    |    |    |    |    |    |
| 19 | Do you manage mobile devices?                    |    |     |    |     |    |    |    |    |    |    |    |    |
| 20 | Are you PCI compliant?                           |    |     |    |     |    |    |    |    |    |    |    |    |
| 21 | Do you have penetration tests?                   |    |     |    |     |    |    |    |    |    |    |    |    |
| 22 | Do you manage configurations?                    |    |     |    |     |    |    |    |    |    |    |    |    |
| 23 | Do you have proper data center environment controls? |    |     |    |     |    |    |    |    |    |    |    |    |
Why is all of this important?

• Less downtime
• Decreases risk to operations
• Lower liability
• Mature processes are more efficient and have better controls
• Lowers total cost of ownership
• On the USB drive
  – White papers
    • How IT Governance Drives Improved Performance
    • Information Technology Standards and Practices for Local Governments
  – Resources
    • Presentation & Summary
    • Twenty Critical Controls for Effective Cyber Defense: Consensus Audit Guidelines
    • California Information Security Strategic Plan (OCT 2009)
    • PCI Resources
    • PCI Presentations
    • ActiveData (Demo)
20+ THE OTHER QUESTIONS TO CONSIDER
Do you have penetration tests?

• A validity test of the vulnerability scans
• Typically finds other attack vectors
• Typical audit findings
  – Don’t know the difference between vulnerability scans and pen tests
  – No penetration tests
• Why is it important?
  – Validate vulnerability scans
  – Vulnerability scans are not 100% accurate
Do you manage configurations?

- Hardware and software configurations
- Laptops, servers, workstations, firewalls, switches, routers

Typical audit findings
- No standard build for configurations
- No documentation
- No validation (continuous monitoring)

Why is it important?
- It is the one that slips through the cracks that is used by attackers
Software Raffle

• Active Data

http://www.informationactive.com/
Contact Info

Tom Lanfranki
CPA, CISA, CIA, CCSA
Information Systems Auditor
Contra Costa County
Office of the Auditor-Controller
tlanf@ac.cccounty.us
Contact Info

Donald E. Hester
CISSP, CISA, CAP, MCT, MCITP, MCTS, MCSE Security, Security+
Maze & Associates
@One / San Diego City College

www.LearnSecurity.org
http://www.linkedin.com/in/donaldehester
http://www.facebook.com/group.php?gid=245570977486