CSMFO Conference 2010

20 QUESTIONS FOR YOUR INFORMATION TECHNOLOGY DEPARTMENT INCLUDING PAYMENT CARD INDUSTRY

No	Question/What is it?	Typical Audit Findings	Why it is Important?
1	**What standard do they use?** - A way to measure your security stance. - NIST, ISO, CoBIT are examples	- No standard used - Not following industry best practices	- How do you prove you are doing what you should be? (Due diligence) - Standards address common risks - Increase 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Licenses - Best to have a continual update process - Perform a full inventory and true up at least annually	- Inventory out of date - No inventory at all - Inventory does not match actual assets (lost or stolen)	- Fines related to missing licenses - Missing equipment (did it contain sensitive data?) - 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	- Audit logs not turned on - If audit logs are turned on, they are not monitored	- Accountability - Proactive approach
4	**Do they control administrative privileges?** - Principle of least access - Access only to what is needed	- Administrative passwords are not changed - Users are local administrators - Information Technology (IT) department users use administrator/root accounts	- 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	- File shares with "everyone" access - More access than needed for job function - Data owners doesn't know who has access to their data	- 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?	- Excessive administrative privilege use - No one knows what Administrators do to systems	- The ability to find incidents during the normal course of business - Proper separation of IT staff duties
7	**Do you have malware defenses?** - Not just Anti-virus - Malware, spyware, adware, virus, worms, popups, Trojans	- 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	- Still a big deal, ability to response to an incident - Downtime - Attackers use this as an attack victor still
8	**Do you have data loss prevention?** - How do you stop data leakage - Information floods out of organizations	- No idea what data loss prevention is: policy, training, etc. - No data loss prevention strategy or data classification - Suffer from the illness that "everything" is public	- Liability (PCI data, HR data, etc.) $$$

Donald E. Hester, Maze & Associates
Tom Lanfranki, Contra Costa County

CSMFO Conference 2010
20 QUESTIONS FOR YOUR INFORMATION TECHNOLOGY DEPARTMENT INCLUDING PAYMENT CARD INDUSTRY

No	Question/What is it?	Typical Audit Findings	Why it is Important?
9	**Do you have an vulnerability assessments?** - What holes do you have in your network? - Know your weaknesses	- No vulnerability scanning - Not following up on vulnerabilities - No internal scanning	- 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	- Access to network is not restricted - Unnecessary service and protocols	- 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	- No incident response capability - No training, no idea what is needed	- 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	- Backups not tested, backup jobs are not configured properly - 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	- 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 upon risk - Protects against excessive and inadequate controls	- No formal risk management process (ad-hoc) - Control selection not based upon risk - Risk and controls are not documented formally accepted by data/process owners	- Don't want to over spend on IT security - Don't want to under spend on IT security
14	**Do you separation of duties?** - Separation of duties in IT tasks as well - Not for all tasks, just critical	- No Separation of Duties (SOD) - No idea of what duties to separate - IT Management doesn't identify single source knowledge experts	- Prevents or limits fraud - Especially on financial systems
15	**How do you manage 3rd parties?** - Get it in writing - Include notification, security requirements and audit	- No formal agreement - No monitoring of 3rd parties - No notification provision - No provision to address data ownership at contract termination	- Your responsibility to protect your data - You can transfer authority not responsibility - If you have a breach with your data don't you want to know ASAP?
16	**Do you have awareness training?** - Initially upon hire, annual classes, regular reminders - Including acceptable use (Internet/Email)	- No ongoing training - Ad hoc, no records of initial training	- Continuous reminder - Just like safety awareness - Limits liability

Donald E. Hester, Maze & Associates
Tom Lanfranki, Contra Costa County

CSMFO Conference 2010
20 QUESTIONS FOR YOUR INFORMATION TECHNOLOGY DEPARTMENT INCLUDING PAYMENT CARD INDUSTRY

No	Question/What is it?	Typical Audit Findings	Why it is Important?
17	**What do you have for wireless security?** - Limit wireless access - On a separate network - Best available encryption	- 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	- It is the easiest way into your network
18	**Do you have application security?** - Security has layers - Don't neglect application security	- Strong network controls weak ERP controls - Audit logs, access control, etc. - Data owners don't know who has access to their data	- If you have a control failure you can still stop an attack - Network controls focus on external threats not internal - Internal fraud will probably include an application
19	**Do you manage mobile devices?** - Control what they connect to when not in your environment - Laptops, phones, USB devices - Encryption	- No control on what connects to your network - No protection if it is stolen	- 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	- Finance thinks it is a IT issue - IT thinks it is a Finance issue - Not compliant	- There is a reason for the controls - Liability $$$
21	**Do you have penetration tests?** - A validity test of the vulnerability scans - Typically finds other attack vectors	- Don't know the difference between vulnerability scans and penetration tests - No penetration tests	- Validate vulnerability scans - Vulnerability scans are not 100% accurate
22	**Do you manage configurations?** - Hardware and software configurations - Laptops, servers, workstations, firewalls, switches, routers	- No standard build for configurations - No documentation - No validation (continuous monitoring)	- It is the one that slips through the cracks that is used by attackers
23	**Do you have proper data center environment controls?** - Safeguards hardware - Laptops, servers, workstations, firewalls, switches, routers	- No environmental monitoring controls (power, temperature, mositure) - No Uninterruptible power supply - No air conditioning	- Heat and power spikes can take out the servers