Chad Ballay

CIS411-342N

Assignment 6-2

**Chapter 6 – Auditing Networking Devices**

**Ensure that appropriate password controls are used.**

* Employees often work remotely and only use their login and password to gain access to the corporate systems.
* Password resets are done by giving out a generic password — *Chiefs2011*.

**Ensure that current backups exist for configuration files.**

* They primarily use Microsoft servers and PCs with a number of Mac computers used to perform design work. They use Active Directory, have a Web Server for their Internet web site, four servers used as file shares (one in each office), four servers housing their architecture applications, a training server, five MS SQL database servers, and two Microsoft Exchange servers for email.
* Each office has its own, decentralized wireless network connected to the production network.
* Onsite staff at each location provides IT support part time along with their other responsibilities.

Identify the job roles of the IT staff that have Network Admin responsibilities. Alignment within this subset of employees will ensure that consistency in policy enforcement will be done.

Identify and review the policies concerning password complexity, reuse, and duration are present and consistent with best practices.

The password reset policy concerns me since it is clearly not ideal. The Director level supervisor of the network admin role would be consulted on industry best practices and the deficiencies present. The work product here would be an acknowledgement and or action plan for process change.

A broad selection or all network devices would be selected for analysis of existing password complexity and uniqueness. Existing password rainbow tables and other tools would be utilized to ascertain weaknesses.

A broad selection or all network devices would be selected for analysis of what mechanism is used for alerting for password changes.

**Chapter 14 – Auditing End-User Computing Devices**

**Verify that systems use a full-disk encryption (FDE) utility to protect company data.**

* They primarily use Microsoft servers and PCs with a number of Mac computers used to perform design work.
* Each employee has a desktop or laptop PC running Windows 7. HR personnel have laptops for conducting interviews.
* Recently, a number of PCs and office equipment has been stolen out of the office.
* It’s at the data owner’s discretion as to whether or not to secure their data files or folders. Many do not *secure* their files, while some lock them so only they have access. There have been rumors that customer data and intellectual property have been lost.

Identify the job roles of the IT staff that have Desktop Support responsibilities. Alignment within this subset of employees will ensure that consistency in policy enforcement will be done.

Identify through the desktop census or document the Network Admin scan the number and variation of desktop devices. The work product for this process is the documentation on how this process can be repeated and the mechanisms for testing validity of the census.

For each desktop configuration the Desktop Support admins will document the process for enabling full disk encryption(FDE) or what other solution they are using. The work product will be a guided document or automated process for enabling this consistently.

The Desktop Support admins will document that administrator level access is needed to enable, modify, or disable FDE. For each modification they will document that an external event log entry was created. If this is not feasible then the Director level supervisor will document acknowledgement and or action plan for implementation.

The Desktop Support admins will document the desktop reporting process for ensuring that existing systems are verified to have FDE enabled. This includes validation checks for rebuilds, os patches, new deployments, and other desktop lifecycle events. The work product is report that can be audited periodically by methodically checking a subset of desktops for compliance vs the reported compliance.

The Desktop Support admin will document how encryption keys are generated, stored, and accessed. Each step of the keys lifecycle will be reviewed for controls and event logging. The work product is the demonstration that each desktop has a unique key, that only appropriate employees have access, and that any access to these keys is logged for possible future review.