CIS-481: Introduction to Information Security

InfoSec Chapter Exercise #4 - Option A

Team: Seven
Participants: Jackson Dillingham, Matt Jackson, Hilton Siaffa, Tabor Payne, and Emily Wantland

Logistics

A. Get together with other students on your assigned team in person and virtually.
B. Review the two options available and decide on only one to pursue as a team.
C. Discuss and complete this assignment in a collaborative manner. Don't just assign different problems to each teammate as that defeats the purpose of team-based learning.
D. Choose a scribe to prepare a final document to submit via Blackboard for grading, changing the file name provided to denote the number of your assigned **Team**.

Problem 1

Explain the differences between a hot site, warm site, cold site and use of a service bureau for business continuity. *(8 points)*

- Warm sites are a step down from a hot site, they provide many of the same services. They do not include the actual applications a company needs, they may be installed, but they won't be configured.
- A hot site is a fully configured computer facility. The site is set up as a working, functioning building complete with duplicate computing resources, peripherals, phone systems, applications, and work stations. Due to the amount of services that a hot site offers, it is the most expensive option for contingency site planning.
- Cold sites are the lowest level of contingency planning sites, but they are the cheapest because they only provide basic services. No computer hardware or peripherals are provided. All services must be installed after the site is occupied. A service bureau provides physical facilities to those who want contingency sites. These agencies typically provide off-site data storage for a fee. Agreements can be signed to guarantee space when needed, if a disaster occurs.

Problem 2

Explain the difference between full, differential, and incremental backup schemes. Be sure to mention what gets backed up each time and how restoration of data would work. *(7 points)*

- Differential backups back up only changed files since the last full backup. This is faster than a full backup, but each daily backup gets larger and larger. A full backup takes a comprehensive snapshot of all the data and information in a system at a point in time. The disadvantage to this method is that it is a large backup and takes a lot of time. The final type of backup is an incremental backup, it captures files that have changed since the last incremental backup. This is a fast backup, but to restore a complete system, multiple backups would be needed. To restore the system, the most recent back up type will need to be accessed and restored onto the servers where the information is stored.

Problem 3
The University of Louisville's Information Security Office maintains the University's information security policies, standards, and procedures. See the overview here:
http://louisville.edu/security/policies/overview-of-policies-and-standards

The current list of policies and standards is here:
http://louisville.edu/security/policies/policies-standards-list

1. From the above list, look for which policy is serving as the Enterprise Information Security Policy (EISP) as discussed in your text. What is its policy number (ISO PSxxx) and name? When did it take effect? How often is it supposed to be reviewed? When was it last reviewed? Is this consistent with the policy's stated timeline for review? *(5 points)*
   - ISO PS001 Information Security Responsibility
   - Effective July 23, 2007
   - Reviewed every year between 2016-2018. These should be reviewed on a yearly basis.
   - Lasted reviewed July 18th, 2018. This is not consistent with the timeline for review.

2. From the above list, look for a policy that would be an example of a Systems-Specific Policy (SysSP). What is the policy number (ISO PSxxx) and name? Is this of the Managerial Guidance, Technical Specifications, or Combination SysSP type? *(5 points)*
   - ISO PS017 Firewalls
   - Combination SysSP. The policy explicitly states the managerial guidance and technical specifications

3. From the above list, look for a policy that would be an example of an Issue-Specific Policy (ISSP). What is the policy number (ISO PSxxx) and name? Is this of the independent, comprehensive, or modular ISSP type? *(5 points)*
   - ISOPS007 User Accounts and Acceptable Use. Modular because each category is split up into different sections.

4. Analyze how the security policies of UofL are implemented on systems to protect a network. Specifically, focus on the following policies and find any weaknesses. *(10 points)*
   - **ISO PS008 Passwords**: The policies in place for passwords are very strong, all user accounts are required to be password protected. Passwords must be reset every 180 days, and each password must be 8-16 characters long and include some type of symbol. This is required to help protect UofL's computing resources.
   - **ISO PS014 Protection from Malicious Software**: These policies are put into place to protect UofL's network from viruses, worms, trojan horses, root kits, and hostile active x controls. Every computer that is connected to the UofL network must have safeguards in place in order to keep malicious software off of the network.
   - **ISO PS017 Firewalls**: Firewalls are put into place to protect central university servers and host systems, all outbound packets are allowed to travel outside of the firewall, and inbound packets are allowed inside the firewall only if they can be determined to be responses to outbound requests.
   - **ISO PS018 Encryption of Data**: All data that is transferred from the university's network must be encrypted. This is implemented because there are thousands of students that use sensitive data that needs to be protected.

- **ISO PS020 Sponsored Acc**ounts: This policy is implemented to protect the university from someone that needs a UofL account that is not a faculty member or staff. In order for this person to receive an account, they must agree and abide by the acceptable use policy.

Problem 4

Compare and contrast the creation and change processes of IETF, ISO, NIST standards? *(10 points)*

- IETF
  - Creation: A specification/standard undergoes a developmental period and through several iterations of review and revisions by the internet community. This involves many formalized documents about the standard. After these steps, it can then be adopted as a Standard by the appropriate organization(s) and is then published. Establishing widespread consensus and evaluating the utility of certain specifications for certain groups are some of the challenges faced during this creation process.
  - Change: When revising a standard with the IETF, we have two options. For the first, it must go through the same steps as creation, and when it reaches completion it will replace the old standard. Sometimes, however, the standards may be used at the same time. These relationships must be explicitly stated. In the second method, the IESG will announce changes which have little community involvement or awareness.
- ISO
  - Creation: Begins with a draft that meets a market need within a certain area. This draft is then shared amongst the appropriate community (usually experts within the specific area the standard is being made for) for comments and discussion. Then the draft is brought to a vote. If the draft is approved, the technical process of creating the standard begins. If the draft isn't approved, then it goes back for comments/discussion until it gets passed.
  - Change: Standards are reviewed at least every 5 years. First, many experts must agree that revision is necessary. The standard goes through review to identify weak points and all parties must reach agreement over the specifications for change. Drafts are then drawn up and reviewed by ISO experts internally. After internal approval, ISO member bodies can comment on the revisions. Finally, these changes are voted upon and revised until majority approval is achieved.
- NIST:
  - Creation: Standards must adhere to internationally accepted principles of consensus, transparency, balance, due process, and openness. Similar to the other two, standards are developed through engagement and discussion with the stakeholders of the standard which includes a public review and comment process. These stakeholders can be in government, industry, or academia.
  - Change: The NIST regularly engages with the community by attending meetings, conferences, etc. as well as receive direct feedback from industry. All the comments/suggestions received are then put into a features list, which prioritizes them based on importance to stakeholders. The NIST then determines if the update is necessary or practical to the stakeholders. If the update is necessary, they the revisions are drawn up and commented upon in the same manner as creation under the NIST.