CIS-481: Introduction to Information Security

InfoSec Chapter Exercise #4 - Option A

Team: 5
Participants: Ethan Grimes, Holli Grubbs, James Hoagland, Gregory Ellis

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)*

A hot site is a facility that contains all the equipment necessary to continue operations in case of an event that causes the main facility to shut down. A warm site is another facility that gives a lot of the same services as a hot site, but usually without installed software apps. With a cold site, it's a facility that provides rudimentary services without computer hardware or peripherals. A service bureau is a continuity strategy where an organization contracts with a service agency to provide BC facilities for a given fee.

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)*

A full backup scheme is the duplication of all files for a whole system. This includes apps, operating systems, and data. With differential backups, it's the duplication of all files that have been added or changed since the last full backup. An incremental backup is the duplication of only the files that have been modified since the last incremental backup.

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)*

Looking at the list above, the policy serving as the Enterprise Information Security Policy is the 'Information Security Responsibility' which has a policy number of ISO-001 v2.0. The policy took effect on July 23, 2007. It is subject to be reviewed yearly and the last time it was reviewed was on January 18, 2021. Based on the policy's stated timeline for review it is not consistent with the policy as it was not reviewed in 2019 or 2020.

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)*

A policy that would be an example of a Systems-Specific Policy would be the 'Security Incidents' which has a policy number of ISO-006 v2.0. This is a managerial guidance SysSP.

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)*

A policy that would be an example of an Issue-Specific Policy would be 'Email Archive' which has a policy number of ISO-019 v2.0. This is a modular ISSP type.

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
        - Passwords that are used on the system are required to follow the standards outlined under the *Technical Standards* section. These standards are used to keep passwords from being compromised. As stated in the section, a few standards include limiting the number of guesses to six, expiring passwords after 180 days, having to be between 8 and 16 characters, and restricting easily guessable words. Upon review of all the standards, the only flaw our group saw is that the minimum number of characters for a password is too low. It should be higher so that it is harder to decipher.
    - ISO PS014 Protection from Malicious Software
        - The University of Louisville provides software security to all computing devices connected to the system. The IT department is in charge of distributing and updating antivirus software, network security, removing infected systems, proper physical layout of the system, and ensuring that the system and any connected device is virus/malware free. The weaknesses our team found are human error and sabotage. People make mistakes and some IT person can accidently put a virus or worse on the system, unintentionally or not.
    - ISO PS017 Firewalls
        - The firewalls protecting UofL's servers and host systems keep the wider Internet from accessing them. Some of the standards include blocking many

different types of network traffic that prove to be harmful to the system, having all internal devices require unique passwords and other appropriate access mechanisms, unique passwords for each firewall, and testing the firewalls on a regular basis. Upon reading the policy, our group found that human error would be the biggest weakness. If a firewall was not properly installed, tested, removed for being outdated, then the system can be accessed.

- ISO PS018 Encryption of Data
  - The encryption of data policy protects the system by encrypting all data, so that it is less susceptible to people outside the system. Some of the standards for this policy include ensuring all computing devices and storage is encrypted, all data backups and passwords are protected, and all data transmitted is encrypted as well. Our group found no issue with this policy.
- ISO PS020 Sponsored Accounts
  - The University of Louisville ensures that all sponsored accounts are only available for people not employed at UofL. This is to ensure that all accounts are for legitimate business purposes with the college only. Some standards include accounts only being requested by a Unit Business Manager and approved by UofL's high ranking officials, ensuring that everyone follows the Information Security Policies, and restricting the user's ability to handle data when necessary. Our group found no issue with these standards.
  -

Problem 4

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

The Internet Engineering Task Force (IETF) instituted new technical documents that influence people to manage the internet. It changes standards based on its participants' engineering judgments and experience with previous implementations of its specifications.

The ISO standards originated from the British Standard BS7799 and evolved over the past 17 years to create the ISO 2700 standards. These standards provide guidelines on how to properly implement information security. The ISO has a "roadmap" for future planned standards that relate to security. These standards evolve as technology becomes more advanced and the threat of cyberattacks increase.

NIST was founded in 1901 and was created with the goal of improving technological infrastructure that the U.S. was falling behind in. NIST standards are reviewed broadly by government and industry professionals that provide guides on how to address information security. NIST also provides a "roadmap" for improving critical infrastructure cybersecurity. The processes change as future developments in technology become more prevalent.