CIS-481: Introduction to Information Security

InfoSec Chapter Exercise #4 - Option A

Team: 1

Participants: Trevor Hagel, Zack Graas, Jacob Forcht

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 *(8 points)*

Explain the differences between a hot site, warm site, cold site and use of a service bureau for business continuity.

A hot site is a fully equipped facility backed up with the hardware, software, and data that the company currently uses. A hot site is configured and ready to go in the event of a failover but it is the most costly of these options. A warm site is a facility with some hardware and some software but no data and it still needs to be configured for failover to happen successfully. A warm site is a step down from a hot site but on the plus side, it costs less than a hot site. A cold site is a facility with power, it's not much but much better than having nothing. A cold site would need a significant amount of setup time and configuration to start conducting business at it. A cold site is really the bare minimum of these sites. A service bureau is a company that provides a business continuity facility for a price. The company would just pay the service bureau and if something were to happen the service bureau would have a facility ready for the company to failover to. The only issue with this is that it is an expensive option.

Problem 2 *(7 points)*

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

A full backup is when the system is completely backed up in its entirety. This takes the longest amount of time and most resources thus is why it typically doesn't occur daily. A differential backup is a backup of all the files that have been added or changed since the last full backup. The size and time are less than a full backup but get larger throughout the week leading up to the next full backup. For restoration, you would load the last full backup and then load the latest differential backup. An incremental backup is a backup of files that have been modified since the last incremental backup. The size and time are less than a full backup and while it's not a consistent amount these backups would be good to do in between full backups. If restoration occurred you would load the most recent full backup and then load all the incremental backups since the last full successful backups.

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)*

The EISP for the University of Louisville is ISO PS-001 v2. It is called Information Security Responsibility. It took effect July 23, 2007. It is supposed to be reviewed yearly. It was last reviewed January 18th 2021, but before that had not been reviewed since 2018.

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)*

One policy that is an example of a Systems-Specific Policy is ISO-017 v2.1. The name of this policy is “Firewalls” This policy is a Combination SysSP because it lists the overall “Administration Standards” of the policy as well as the “Technical Standards” expected.

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)*

ISO PS-007 is an Issue-Specific Policy. It is named “User Accounts and Acceptable Use” and it guides IT security on the standards for organization user accounts. It is an independent ISSP.

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

UofL uses passwords to make sure that the right users have the right permissions and access to the network. UofL’s ISO PS008 Passwords policy has good password standards but something that it lacks is two-factor authentication. If someone fell victim to a phishing attack and entered in their username and password the bad actor could get into the system and get access to the network. Two-factor would add an extra layer of protection.

- ISO PS014 Protection from Malicious Software

UofL uses antimalware software to detect malware and remove malware from systems that could infect the network. The issue here is that a user could connect to the network without their antivirus software activated. The standards say that antivirus software must be installed before connecting but I do not see any controls for making sure this is occurring. Windows defender is really easy to disable as well. If the antivirus software is disabled this could allow malware to infect the network which is a security risk.

- ISO PS017 Firewalls

UofL uses firewalls to protect its Network from the open internet. UofL does this by only allowing certain addresses and automatically blocking traffic from certain ports.

- ISO PS018 Encryption of Data

UofL wants all users to have encrypted data to protect the data on the network. Encryption is also good protection in case of theft if any thief tries to access private data it won’t be easily accessed. Also, any data transmitted across the network should be encrypted to protect it.

- ISO PS020 Sponsored Accounts

UofL has created specialized sponsor accounts to give sponsors a way to interact with UofL's network in a safe way. These accounts have limited permissions to make sure that they can't interact with UofL's network in a malicious way. This policy is also to make sure that these accounts are only given to valid businesses or academic relationships that require accounts. This so that we only give these special accounts to people who need them.

Problem 4 *(10 points)*

Compare and contrast the creation and change processes of IETF, ISO, NIST standards?

One way that these three standards are similar is in the way they do their processes. The IETF standard has a straightforward process where they go through and review several iterations by a community on the Internet. The ISO used a group of people from many organizations to help with things that they have expertise and wisdom in working on. Finally, the NIST works with the government to come up with solutions for organizations in the government. For example, they worked with homeland security and information technology. They work with the government to improve technology and take care of standards. The creation of these three standards was very different. The ISO starts with a few delegates from different countries to talk about standards on an international level. The NIST started as a place to create standards for science-based technologies. As for IETF standards, it was created to help the Internet be able to operate, manage, and evolve itself. Also, it was helped by several other groups like the Internet Society aka the ISOC.