CIS-481: Introduction to Information Security

In-Class Exercise #4 - Option A

IQ Team: 4
Names of team members: Daniel Kearl, Mohammed Al Madhi, Yuxuan Chen, Joseph Baxter

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 **IQ 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)*

All the mentioned sites are different physical locations than the live production site, with varying degrees of operability and preparedness. A hot site is the most prepared and operable of them all, as it is essentially a mirror image of the production site, potentially only lacking access to live data and the people required to run operations at the site. The idea is that a hot site should be up and running with very little to zero service downtime; as one might imagine, this is a very expensive but also crucial asset to an organization that cannot tolerate downtime.

A cold site is on the opposite end of the operability and preparedness spectrum. These have almost nothing set up and ready for operation, including any computers, networking, etc. Cold sites are essentially just empty buildings with only basic utilities like electricity, where everything necessary to facilitate operations would need to be set up in the situation that the site was needed. While this isn't very helpful for downtime prevention as-is, it is a very cheap stepping stone to having a backup site running.

A warm site is somewhere in the middle of hot and cold, as one would imagine. Generally, these sites have servers and other equipment available, but not configured or ready for operations. Client workstations are absent, and as a result, much more work and time is required to get a warm site up and running, but not as much work or time as it would to prepare a cold site. As with its preparedness, the price of a warm site is also somewhere in the middle, aligned about with how prepared the site is for operations.

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 of a disk is just what it sounds like: it saves a complete copy of the entire disk's contents, usually in the form of a disk image. Due to their completeness, these backups occupy the

most storage space and take the most time to run when compared to other types of backups, so the are used a bit less frequently. These are usually scheduled to occur during lulls in system usage (like weekends), because in a large computer system, all machines would be hit at once with a backup job, potentially reducing performance if someone were using that system at the time. These do have a massive benefit over the other backups; they can be used to completely restore a system to its saved state without referencing anything else.

Differential backups can be seen as a step down from full backups in that they don't back up the entire system, only any changes made since the last full backup. This means as the time that has elapsed since the last full backup increases, so will the size of the differential backup, and the time it takes to complete the backup. Restoring a differential backup requires the differential backup and the last full backup, which means any previous differential backup can be corrupted or lost with no impact on restoration.

Incremental backups are usually the smallest and fastest form of backup, because these only save any changes made since the last incremental backup (or other backup if it is the first one of its kind created). These require the least space and can be done the fastest, resulting in them being run much more often in an organization environment. The downside here is a corrupted incremental backup will be an issue when it comes to restoring a system.

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 policy acting as the EISP seems to be the Information Security Responsibility policy (ISO PS001). It took effect on July 23, 2007 and was last reviewed and revised on July 18, 2018 (version 2.0, updating grammar and punctuation). The policy itself states that it should be reviewed annually, and seeing that the last review was in 2018, it does not seem to be consistent with its review timeline.

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 notable SysSP we found was the Firewalls policy (ISO PS017). It seems to be a combined managerial *and* technical type of policy, because there are administrative standards covered alongside specific technical standards.

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)*

An ISSP in the above list is the Network Service policy (ISO PS010). Based on the different categories covered and the detail in which they are covered, the policy seems to lean toward a comprehensive 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
    - ISO PS014 Protection from Malicious Software
    - ISO PS017 Firewalls
    - ISO PS018 Encryption of Data
    - ISO PS020 Sponsored Accounts

Security policies are implemented firstly by policies and guidelines, and secondly by actual limitations to prevent actions that are outside anything specified in those policies. For example, the Passwords policy (PS008) states, among other things, that no password should contain the user's ID or name. This is reinforced by the system that allows you to change passwords not actually *allowing* someone to set a password with these characteristics.

We did find a relatively outstanding weakness in the Passwords policy (PS008). This policy states that any password to systems containing sensitive information must follow three of four criteria listed, but we believe this would be more secure without giving up much if all four criteria must be followed.

Problem 4

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

In terms of creation, IETF takes recommendations from inside working groups that suggest initiation of action toward implementing a standard. ISO on the other hand has a system of implementing a standard that begins with a proposal, then preparation of a working draft that is shared with ISO members before revision and finalization. NIST is similar, as the organization is very formally and rigidly established, and was one of the first to establish such standards.

As for changing standards, the IETF will submit the revised standard as if it were a new standard entirely, and if it is improved it will replace the old standard. NIST and (especially) ISO standard changes are revised rather than replaced, and are audited thoroughly both internally and independently, before they are finalized and put into place for other organizations to follow.