CIS 481 – Intro to Information Security

IN-CLASS EXERCISE # 4

Names of team members: **Trisia Baltazar, Adrian Boone, Savanah Kennedy, Ryan Smith**

Logistics

A. Get into your regular team

B. Discuss and complete the assignment together. Don't just assign different problems to each teammate! That defeats the purpose of team-based learning.

C. Choose a recorder to prepare the final copy to submit to instructor in Blackboard.

Problem 1

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

A hot site is a fully configured computer facility with all services, communications links, and physical plant operations. It duplicates computing resources, peripherals, phone systems, applications, and workstations. It is the pinnacle of contingency planning and is the most expensive as it is reliable and used if an organization needs 24/7 capability for near real-time recovery.

A warm site provides some of the same services and options as a hot site, but does not include the actual applications the company needs. They include computing equipment and peripherals with servers, but not client workstations. It is cheaper than a hot site and requires hours or days to be fully functional.

A cold site provides only rudimentary services and facilities. No computer hardware or peripherals are provided. It is basically an empty room with heating, air conditioning, and electricity. Everything else is an option. The main advantage of a cold site is that it is much cheaper.
A service bureau provides business continuity because if a disaster were to happen, a bureau would provide physical facilities and frequently provide off-site data storage for a fee. The disadvantage to this is that it is a service and must be renegotiated periodically and can be expensive.

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 pts.)

Full backup: A full backup is exactly what it sounds like - it's a complete and comprehensive backup of your entire data set, including applications and OS components. Full backups provide the best protection against data loss, since absolutely everything is backed up, but they are particularly time-consuming and require a large amount of storage media to retain the backup data. Restoration from a full backup is simple, since you only need the one full backup to restore from, instead of multiple such as with differential and incremental backups.

Differential backup: A differential backup is a backup that updates the full backup's data set only with the files that have been changed since the last full backup. This method requires less storage space than a full backup and is also faster to restore, but as time progresses, each new backup will be larger and slower than the one previous. A system restoration using differential backups would involve the use of both the original full backup and the most recent differential backup.

Incremental backup: An incremental backup is similar to a differential backup, but it only backs up the data that has changed since the last *incremental* backup, instead of the last full backup. This keeps both storage space and cycle time lower than it would be for a differential backup. In the event of a restore using incremental backups, you would need each preceding incremental backup - if you made a full backup on Monday, and wanted to restore to an incremental backup you made on Thursday, you would also need the incremental backups for Tuesday and Wednesday.

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 pts.)

ISO PS001 Information Security Responsibility serves as the Enterprise Information Security Policy (EISP). We came to this conclusion, because it is a general security policy and shaped the philosophy of security in the IT environment of UofL. The responsibilities of various areas of security, including systems administrators and providers, maintenance of the information security policies, and the practices and responsibilities of users are all addressed in this policy. This almost entirely covers the book's definition of an EISP. It took effect on July 23, 2007. It is supposed to be reviewed annually. It was last reviewed on June 12, 2017. The time it was reviewed before that was March 8, 2016. It is consistent with the policy's stated timeline for review. It should, however, be reviewed again soon.

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? (3 pts.)

ISO PS017 Firewalls is an example of a Systems-Specific Policy (SysSP). This is of the Combination SysSP type, because it has a section dedicated to Administrative standards (which is of the

Managerial Guidance type) and has a section dedicated to technical standards (which is of the Technical Specifications type).

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? (2 pts.)

The policy number is ISO PS008. The policy name is Passwords. This is an example of the independent ISSP type.