CIS 481 – Intro to Information Security

CLASS EXERCISE # 4

Problem 1

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

- There are many differences between hot, warm, and cold sites. To begin, 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. Warm sites are a step down from a hot site. They provide many of the same services that a hot site provides. However, it does not include the actual applications the company needs, or they may be installed, but not configured. Cold sites are the lowest level of contingency planning sites, but they are the cheapest. Cold sites 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 pts.)

- There are three different types of backups. 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. 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. The final type of backup is an incremental backup, which 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 access, and restored onto the servers which 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 pts.)

- The policy number for the EISP of the University of Louisville is ISO PS001 and named Information security responsibility. Its effective date was July 23, 2007. The policy is reviewed annually. It was last reviewed on June 12, 2017. According to this timeline, it is consistent through the last two years, and to remain consistent, should be reviewed presently in 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? (3 pts.)

- ISO PS010 is the policy number and it has been named "Network Service." It is both a managerial guidance and technical specification policy.

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.)

- An example of an ISSP is policy number ISO PS008 called Passwords. This is an example of a comprehensive ISSP because it is a comprehensive policy, written by management, that establishes guidelines for overall coverage of necessary issues.