CIS 481 – Intro to Information Security

IN-CLASS EXERCISE # 4

Names of team members: Volodymyr Bestiyanets, Nick Cunningham, Timothy Mahan, and Shawn Nasr.

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.)

Business continuity involves the use of hot sites, warm sites, cold sites, and the service bureau. A hot site is a completely configured computing facility that consists of all services, communication links, and physical plant operations. They duplicate computing resources, peripherals, phone systems, applications, and workstations. A warm site is a facility that utilizes most of the same services as a hot site, at a lower cost, with the exclusion of software application installation and configuration. It commonly includes computing equipment and peripherals with servers without client workstations. A downside of a warm site is that they typically take hours or even days to become fully functional. A cold site is a facility that covers the most basic services, without any computer hardware or peripherals. A cold site can be cheaper than hot and warm sites, though, leasing a new space could be more convenient than maintenance fees for a cold site. Service bureaus is a contractual agreement with a service agency to provide a business continuity facility, typically off-site, in the event of a disaster for varying fees. This can benefit an organization by meeting their specific needs without having to reserve dedicated facilities. The downside of a service bureau is that the price of service will have to be renegotiated from time to time and be costly.

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.)

The three different types of backup schemes include full, differential, and incremental backups. A full backup is almost exactly what it names suggests, a very detailed backup of a systems data and information. As detailed an extensive this backup technique may be, it is also extremely expensive and time consuming. Companies with high priority information to their operation may consider periodic full backups. Two alternatives to a full backup option include differential and incremental backup’s. A differential backup only backs up the change in information from the previous full backup. If a full backup was performed on Monday then the differential backup would include everything recorded on Tuesday and Monday’s backup. An incremental backup only records information that has changed from the last incremental backup. As far as the priority of information goes, information with the highest priority should receive periodic full backups. Information with the next highest priority should receive differential backups while information with the least priority should be backed up incrementally. Backup information should be stored at offsite locations and backups should be performed at night to prevent the least amount of interference.

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/iso-policies/policies-standards-index

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 serving as the EISP is ISO PS001, Information Security Responsibility. It took July 23, 2007. This policy is supposed to be reviewed annually to ensure the policy is in compliance with applicable security regulations and University direction. This policy was last reviewed March 8th, 2016. This is inconsistent with the policy's slated timeline for review.

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.)

From the list of policies, an example of a Systems-Specific Policy (SysSP) would be the "Firewalls – IT Division Policy", ISO PS-017 v2.0. It is a SysSP because it is associated with the standards to be used when configuring and/or maintaining systems. This policy is a combination SysSP because it combines the managerial guidance and technical specifications into a single document. There is an administrative section that is utilized to guide behavior of employees to properly implement and configure the technology used. The technical specifications in this policy outline the configuration rules for the systems firewalls, indicating how the security system will react to the data it receives.

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 issues specific policy would be the ISO PS019, Email Archiving. This policy is of the independent type as this and other policies are created and maintained by different groups, and each policy is written about a specific issue.