CIS-481: Introduction to Information Security

InfoSec Chapter Exercise #4 - Option A

Team: 3
Participants: Brandon Crosier, Marvin Weaver, Kitrina Justus, Sam Steele, Aaron Gordon

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

A hot site is an off-site computer facility that is fully configured with all services, communication links, and physical plant operations. This type of site is the most expensive as it is basically a copy of the current facility, down to the software download. A warm site is a facility that provides many of the same services that a hot site does, but without installed and configured software applications. A warm site provides many of the same capabilities as a hot site but at a lower cost. A warm site also requires much less set up time and is operational much faster than a hot site. A cold site is a facility that provides rudimentary services, with no computer hardware or peripherals.

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 is the duplication of all files for an entire system, including all applications, operating system components, and data. This type of backup essentially takes a comprehensive snapshot of an organization's system. Differential backup is the duplication of all files that have changed or been added since the last full backup. Incremental backup duplicates only the files that have been modified since the previous incremental backup. The first step in the backup and recovery system is scheduling and storing the backups, usually done daily, onsite for incremental and differential backups, and weekly, offsite for full backups. Typically, all backups are done overnight when system activity is lowest and the risk of user interruption is low.

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 serving as the EISP is the Information Security Responsibility, policy number: ISO-002 v2.0. This policy has been in effect since July 23, 2007. The University states the policy is reviewed annually to determine if the policy addresses University risk exposure and is in compliance with the applicable security regulations and university direction. It also states that changes only take place if the policy no longer complies with the university's security standards. The most recent review date was May 18, 2018. This information is not consistent with the policy's review dates.

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)*

The policy serving as the Systems-Specific Policy is Security Incidents, policy number: ISO-006 v2.0. This policy includes a combination SysSP type (Managerial guidance and technical specifications) because standards and procedures are outlined in the 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? *(5 points)*

An example of an issue-specific policy is the Email Archive Policy, policy number: ISO-019 v2.0. The policy accounts for the time period (120 days, 2 years, 5 years, 7 years etc) emails are archived for, based on their data type. This policy is of the modular ISSP type because it is customized to individual technical issues i.e. the data types.

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

The ISO PS008 Passwords policy protects the network by requiring long, complex passwords for any website containing sensitive information. They also require an encrypted database to hold the passwords, not a hardcopy or plaintext version. A weakness of this one could be a brute force attack if they got lucky as they allow for six attempts before locking. A dictionary attack couldn't work because they don't allow users to use passwords solely from a dictionary or commonly used phrases. A rainbow table could work if the hacker has access to the encryption file. The easiest way for the hacker to get the password information would be through a social engineering attack since the university has so many protections in place.

ISO PS014 Protection from Malicious Software protects the network by requiring antivirus software and removing all infected devices from the network. Unfortunately, the weakness in that is that the infected device will have to be detected first, meaning the network is likely already infected. Fortunately, they also have firewalls in place in case anything does try to attack the network.

ISO PS017 Firewalls protect networks by mandating firewalls to be placed on every device on the network. This makes it harder for hackers to access sensitive information. Unfortunately, not all students will place firewalls on their personal devices as it may limit some of what they can do, leaving both them and the network open to attack.

ISO PS018 Encryption of data protects the network by ensuring data is protected through encryption and backups in case anything should happen to the data. Since the data is encrypted, it is well protected, but not foolproof. Anyone who gets access to the encryption key can then access the data. However, the university has issued standards that would make it hard for anyone to get access to the encrypted file alone, let alone the encryption key. Someone inside the organization would have an easier time getting this information, so proper practices of employees and screening of new hires would be a must.

ISO PS020 Sponsored Accounts protects the network by requiring all those requesting to be approved and agree to the acceptable use policy of the university. Since the account must be approved by a superior, it is unlikely that anyone with malicious intent will gain access unless they are a social engineer infiltrating the trusted UofL affiliate as well.

Problem 4

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

The ISO, international organization for standardization, model is one of the most widely referenced security models. It presents a standard information security framework that states the organizational security policy is required to give management direction and support. ISO gives recommendations for information security management and acts as a starting point for the development of organizational security. If a change is determined to be necessary by the industry or businesses, then an implementation period will be allotted allowing users to decide what to do about the change.

NIST or the National Institute of Standards and Technology creates security models that support the mission of the organization and are an integral element of sound management.

The security should be cost-effective because most owners have other security obligations outside of the organization. Also, security responsibilities and accountability should be made explicitly clear because security requires a comprehensive and integrated approach. To create new standards NIST has a framework that consists of 3 fundamental parts and they are the Framework Core which is a set of infosec activities that an organization is expected to perform and their desired results. The next fundamental part is framework tiers which help to relate the maturity of security programs and implement corresponding measures/ functions. The last fundamental profile which is used to perform a gap analysis between the current and the desired state of info security. To change a standard NIST has a 7-step approach.

IETF, or Internet Engineering Task Force, is used to produce technical documents that describe internet standards. The process for resting a standard starts with development and review. The standard requires several iterations to be presented before a committee and must be revised by them before it is published. In order to change an existing standard, an appeal must be made to the community. The community then decides whether it is a valid or invalid request.

All of them have an approval process for changes. The difference between them is that IETF allows any community member to suggest a change while the other two only permit industry and business partners to suggest changes. They all act as pillars of the information security model community, they just target different audiences. While IETF is for engineers specifically, NIST and ISO support management.