CIS-481: Introduction to Information Security

InfoSec Chapter Exercise #4 - Option A

Team: 6
Participants: Regis Wilson, Kelsey Beeler, Mahendra Khanal, Anthony Combs

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 office that is completely configured. This implies that actual activities, correspondences and administrations are running and all set. A hot site is the costliest site to run. A warm site has similar administrations as a hot site, however the product isn't introduced and arranged. A virus site offers just simple types of assistance. These destinations don't have any equipment or peripherals. A cold site is the least expensive site out of the three locales. Hot, warm and cold locales are totally utilized for business congruity tasks. An assistance agency is utilized for business coherence by consenting to give an actual office to an association if there should be an occurrence of a fiasco. These authorities can likewise give off-site information stockpiling if the association pays an expense. The objective for utilizing these agencies is to consistently have a back-up for information just as a spot to run the associations activities if there should be an occurrence of a fiasco. An issue with administration agencies is they resemble protection and can be pricey.

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 a finished duplicate of all information. This is the most secure reinforcement however requires a ton of time and a ton of circle space. This can be exorbitant. You can simply utilize the full update, however on the off chance that it isn't the most recent reinforcement, you should utilize one of the accompanying. A steady reinforcement duplicates all the information that has changed or been added since the last reinforcement. This permits all

information to be made sure about yet rebuilding can become tedious, as every reinforcement should be recuperated each in turn. When stacking up gradual reinforcements you need the full back up just as all steady reinforcements that are not ruined or harmed. A differential reinforcement duplicates all the information that has changed since the last full reinforcement. This is gradual, yet rather there would just be two focuses to reinforcement, making reclamation quicker than steady. The disadvantage, the differential reinforcement can develop to be very huge. Differential reinforcements need the full reinforcement, yet just need the most recent practical differential reinforcement to reestablish the framework.

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)*

ISO-001
V2.0
Effective: July 23, 2007
Information Security Responsibility
It has been reviewed once a year, in different months for the years 2016, 2017, 2018, and 2021. Last reviewed January 18, 2021. The policy states its to be reviewed annually.

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)*

Name: Workstation and Computing Device
ISO-012
Effective: July 23, 2007
Technical Specifications

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)*

Policy Name: Security Incidents
This is a Comprehensive ISSP type because it is covering all issues that relate to potential security incidents
July 23rd, 2007
Policy Number: **ISO-006** Version 2.2

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

PS008 is used to protect users because information needs to be kept confidential an in order to do that with a strong password must be created, only one person with knowledge of that password (the user), no sharing of password, and passwords that has been suspected or compromised needs to change right away. one weakness would be if a user did not change their password every so often, not choosing a strong password that has bare minimum specifications or a similar password to their last one another weakness is if a antivirus is not often used on personal devices and is not detected or removed. Or setting up the firewall incorrectly, or not having no firewall at all. Upon looking at the other policies (PS014, PS017, PS018, and PS020), we see that one potential weakness for all of them could be the reliance on a Microsoft system that as we know is not completely, 100% reliable and if that system goes down then everything would be left vulnerable. Other than that weakness, none of them presented to have any outstanding weaknesses that stand out to any of us.

Problem 4
Compare and contrast the creation and change processes of IETF, ISO, NIST standards? *(10 points)*

IETF (Internet Engineering Task Force) - Is another open source that promotes internet standards. The most notable standard makes up the internet protocol suite. It is run by volunteers and has no formal organization.

ISO Information Technology – Code of Practice for Information Security Management. This was originally published as British Standard BS7799. When it was adapted as an international framework by the international Organization for Standardization

(ISO) and the International Electrotechnical Commission (IEC) it was renamed ISO/IEC 17799. This is a serious of documents focused on giving a broad overview of various information security issues. It addresses 14 security control clauses, 35 control objectives, and over 110 individual controls. The document was mainly used in the UK.

NIST - Is a publicly available source of documents from the NIST Computer Security Resource Center. These documents are available at any time at no charge. The United States Government have cited several of these documents when getting ruling or setting standards. It is also a popular source for industry professionals and academics.