IS 497B: Information Security and Assurance
Course Project
Creating a Corporate Information Security Plan

Introduction

This project is designed to complement the IS 451 Systems Development Project course. This is a group project for which your group will create a corporate information security plan based on the company profile that you, or others in your group, developed as part of the requirements for the IS 451 course. You do not need to be taking, have taken, or even plan to take IS 451 to be able to participate fully in, and complete, the project. The IS 451 project will simply provide the background industry and company analysis, enterprise resource planning proposal, and functional area system module rollout proposal that is the basis of your information security plan.

There are two documents to be produced for this project. One has two parts to it. The first part is drawn from the company profile from the IS 451 project. It should be a summary of the company that your group is building the InfoSec plan upon. The discussion in this part needs to provide enough information to clearly define the enterprise information architecture as well as the challenges the environment presents such as the regulations the company has to adhere to and what sensitive data and information the company must manage and what standards that need to be met. That discussion will lead to the second part of this document that will be a discussion of the various InfoSec planning documentation your group has selected, including the models you have selected for your InfoSec Plan, with the rationale for those selections. You need to be sure to cite all sources used.

The other document is what I refer to as the "presentation" document. It contains the formal InfoSec plan for your company. Not that you will be presenting the document, but that it is a finished document such that could be presented to the Board of Directors as the company's formal InfoSec plan. Therefore, the formatting of this document should be whatever your group deems appropriate for such a document (of course, I will ultimately determine the appropriateness of the format as part of the scoring rubric). As discussed in class, you do not have to generate original content for the InfoSec Plan document. You do not even need to paraphrase your sources. You may simply copy the source and modify the content to fit your company. The only concession to academic form, therefore, is for you to carefully cite all of your sources. You may use any reasonable citation format you wish (I will ultimately determine the reasonableness of the citation format) so long as you include complete citations. I suggest you footnote, endnote, or provide a numbered list of reference that are then indicated throughout the document. Also, avoid using URLs in the citation unless the source is available only online—if there is a volume and issue number, then use that, even if you found it online. Also, do not use the URL resulting from a search engine; use the direct link URL.

Finally, you will need to bind the two documents together. There needs to be some form of divider or tab to separate the two documents (other tabs and dividers may be used as you see fit). The binding may be a three-ring notebook binder or other method of your choosing, but whatever you choose, I should be able to open the document flat.

Overview

The materials drawn from the IS 451 project are necessary for this project and parts of some of the documentation from that project and summaries of some sections will be included in the documentation for this project. While the IS 451 project documentation is necessary, it is not included in the scoring rubric for this project. However, failure to include part or all of the documentation or providing substandard analyses and proposals can affect the score your group receives on the project. Then your real project for this course begins. Provide documentation of a comprehensive information security strategy for your company.

Information Security Plan

Develop an information security plan based on the company information that is appropriate for the company and the industry in which it operates. Begin with the enterprise information security plan (EISP) that will serve as an overview of the organizational philosophy on information security. This will require your group identify a standard appropriate for the company and the industry in which it operates and to develop a hybrid model that will enable the company to meet its security goals. The EISP needs to describe risk management in terms of how the organization deals with risk, what methods the company uses (or should use) to identify risk and perform a top-level risk analysis/assessment. The EISP should also describe the SETA program and included the contingency plan. Following the EISP will be the issue-specific security plan (ISSP) that addresses areas of information security policy that apply to the entire organization. Then systems-specific security policy (SysSSP) will be developed for the functional area system module described in the IS 451 project documentation.

Project Checklist

What follows is a checklist of the components that will be contained in your project documentation and should serve as a guide for the major headings of your presentation. This list comprises the items that should be part of any InfoSec Plan but may not reflect all components that should be part the plan for your company. Greater detail of the content of the project documentation and how it should be presented will be provided as the term progresses.

- Cover Page – in the jacket of a vinyl three-ring binder
- Table of Contents
- Company Background/Description (From the IS 451 Project)
  - Executive Summary
  - Industry Analysis
  - Company Analysis
  - Organization Chart
    - Place IS and InfoSec Management in the organizational hierarchy
- Enterprise Information Security Plan (EISP)
  - Overview of organizational philosophy on information security
  - Structure of InfoSec organization and individuals who fulfill InfoSec roles
  - Articulate security responsibilities for all entities of the organization
  - Including contractors and business partners
  - Articulate responsibilities unique to each role in the organization

- Articulate Information Security Strategy
  - Purpose
  - Organizational Security Strategy Statement
    - Tantamount to Security Mission Statement
  - Define or describe the model standard
- Risk Management
  - How the organization deals with risk
    - Appetite
    - Strategy
  - Define/describe methods for identifying risk
- SETA Program
  - Definition and Purpose in the EISP
  - Organizational commitment to SETA
  - Level of education, training and awareness
  - How security education, training and awareness will be disseminated throughout organization
- Contingency Planning
  - Definition in the EISP
  - Level of preparedness
  - Response to contingencies
  - Continuity of operations

- Issue-Specific Security Policy
  - Address the prominent issues of information security that you can reasonably determine the organization faces.
  - Example ISSP topics
    - User accounts and passwords
    - Computer and internet usage
    - Database and network access
    - Level of surveillance
  - SETA program
    - Description of components program in the ISSP
    - How security education, training and awareness affects specific issues
- System-Specific Security Policies (SysSSP)
  - For the functional system module identified in you IS 451 project
  - SETA program
    - Description of security education, training and awareness for system users
  - Risk Analysis/Assessment – document the:
    - Identification of information assets
    - Valuation of information assets
    - Vulnerability of those assets
    - Identify baseline controls
    - Identify residual risks and means of eliminating it.

Some Things to Keep in Mind

- Avoid absolute wording or guaranties
  - e.g., Best, totally secure, etc.
    - May create a standard no one can live up to
    - Thus, opening the organization to liability if you're not "perfect"
- Avoid describing unrealistic levels of security
  - Due care does not require perfection
  - Rather, due care requires prudent efforts at security
- Avoid details
  - Policy is a top-level governing document
  - Not detailed instructions
- Be sure to identify the standard
  - Make sure it is appropriate for your organization and the industry it works in