NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

ANALYSIS OF SECURITY SOLUTIONS IN LARGE ENTERPRISES

by

Carmen F. Bailey

June 2003

Thesis Advisor:	Paul C. Clark
Co-Advisor:	Cynthia E. Irvine

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** June 2003	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Analysis of Security Solutions in Large Enterprises			**5. FUNDING NUMBERS**
6. AUTHOR(S) Carmen F. Bailey			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT ***(maximum 200 words)***

The United States Government and private industry are facing challenges in attempting to secure their computer network infrastructure. The purpose of this research was to capture current lessons learned from Government and Industry with respect to solving particular problems associated with the secure management of large networks. Nine thesis questions were generated to look at common security problems faced by enterprises in large networks. Research was predominantly gathered through personal interviews with professionals in the computer security area from both the public and private sector. The data was then analyzed to compile a set of lessons learned by both the public and private sector regarding several leading computer security issues. Some of the problems were challenges such as maintaining and improving security during operating systems upgrades, analyzing lessons learned in configurations management, employee education with regards to following policy and several other challenging issues. The results of this thesis were lessons learned in the areas of employee education, Government involvement in the computer security area and other key security areas. An additional result was the development of case studies based upon the lessons learned.

14. SUBJECT TERMS Analysis of Large Enterprise Systems			**15. NUMBER OF PAGES** 99
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

ANALYSIS OF SECURITY SOLUTIONS IN LARGE ENTERPRISES

Carmen F. Bailey
Civilian, Naval Postgraduate School
B.S., University of Richmond, 1996
M.S., Boston University, 2001

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
June 2003

Author: Carmen F. Bailey

Approved by: Paul C. Clark
Thesis Advisor

Cynthia E. Irvine
Co-Advisor

Peter J. Denning
Chairman, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The United States Government and private industry are facing challenges in attempting to secure their computer network infrastructure. The purpose of this research was to capture current lessons learned from Government and Industry with respect to solving particular problems associated with the secure management of large networks. Nine thesis questions were generated to look at common security problems faced by enterprises in large networks. Research was predominantly gathered through personal interviews with professionals in the computer security area from both the public and private sector. The data was then analyzed to compile a set of lessons learned by both the public and private sector regarding several leading computer security issues. Some of the problems were challenges such as maintaining and improving security during operating systems upgrades, analyzing lessons learned in configurations management, employee education with regards to following policy and several other challenging issues. The results of this thesis were lessons learned in the areas of employee education, Government involvement in the computer security area and other key security areas. An additional result was the development of case studies based upon the lessons learned.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

This author would like to acknowledge the National Science Foundation for the opportunity to attend the Naval Postgraduate School under the Federal Cyber Service Corps Scholarship for Service Program.

This author would like to acknowledge the financial support of the National Science Foundation for allowing the purchase of materials used in support of this thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

The United States Government and private industry are facing some adversity in attempting to secure their computer network infrastructure. There exists an ever-growing challenge to try and keep pace with the security issues that arise as technology changes. Large networks can exchange vast quantities of information over a global scale and more and more people and becoming dependant on computer technology. While this is a positive tool for organizations to exchange data in this manner, it also leaves the public and private sector vulnerable to attacks by malicious users. The purpose of this research was to capture current lessons learned from Government and Industry with respect to solving particular problems associated with the secure management of large networks.

The research questions presented in this thesis are derived from the Internet, periodicals, text readings and classroom discussions regarding computer security. There are eight primary thesis questions followed by one secondary thesis question. The nine questions represent some of the more common challenges faced today in the attempt to secure large systems. The intent behind the selection of these questions was to generate lessons learned from common computer security problems encountered in the public and private sector.

The questions are as follows:

Primary Questions

- What effect does a major operating system upgrade have on the security of a large enterprise?
- Given a large installation of computers, how can their configuration be managed in a consistent and secure manner?
- Given a large installation of computers, how can the myriad of possible configuration options be set to support a secure configuration, which satisfies a given policy?
- Given a large enterprise, how can the large amounts of audit data be efficiently handled, monitored, and backed up?
- How can large amounts of data spread over many systems be quickly and effectively destroyed? (emergency destruction)

- How can large amounts of backup data be quickly recovered?
- How can large amounts of data (Terabytes) be properly handled in support of forensic and/or prosecution activity?
- How can we effectively convey the importance of following policy to employees of a large enterprise to specifically combat social engineering?

Secondary Question

- How can current Government and private sector computer security issues be applied through case study analysis to the education and preparation of the Department of Defense computer security workforce?

Research was predominantly gathered through personal interviews with twenty-seven computer security professionals from both the public and private sectors. The many answers to the questions listed above were then analyzed to compile a set of lessons learned. The results of this thesis were lessons learned in the areas of employee education, Government involvement in the computer security area and other key security areas. An additional result was the development of educational case studies based upon the lessons learned.

I. INTRODUCTION

This thesis analyzed real-world questions surrounding a number of security problems affecting large enterprises, such as those encountered by the United States Government and private industry. The approaches that these organizations took to try and solve these problems, as well as commonalities and differences that these approaches had when solving a particular class of problem were investigated. Some of the problems were challenges such as maintaining and improving security during operating systems upgrades, analyzing lessons learned in configurations management, employee education with regards to following policy and several other challenging issues. The results of the research are applied to support the Naval Postgraduate School's Computer Science (CS) Secure Management of Systems course.

A. QUESTIONS TO ANSWER

The questions presented in this thesis are derived from the Internet, periodicals, text readings and classroom discussions regarding computer security. There are eight primary thesis questions followed by one secondary thesis question. The nine questions represent some of the more common challenges faced today in the attempt to secure large systems. The intent behind the selection of these questions was to generate lessons learned from common computer security problems encountered in the public and private sector.

The questions are as follows:

1. Primary Questions

- What effect does a major operating system upgrade have on the security of a large enterprise?
- Given a large installation of computers, how can their configuration be managed in a consistent and secure manner?
- Given a large installation of computers, how can the myriad of possible configuration options be set to support a secure configuration, which satisfies a given policy?

- Given a large enterprise, how can the large amounts of audit data be efficiently handled, monitored, and backed up?
- How can large amounts of data spread over many systems be quickly and effectively destroyed? (emergency destruction)
- How can large amounts of backup data be quickly recovered?
- How can large amounts of data (Terabytes) be properly handled in support of forensic and/or prosecution activity?
- How can we effectively convey the importance of following policy to employees of a large enterprise to specifically combat social engineering?

2. Secondary Question

- How can current Government and private sector computer security issues be applied through case study analysis to the education and preparation of the Department of Defense computer security workforce?

B. SCOPE OF RESEARCH

This thesis presents data gained through the collection and analysis of United States Government entities and large enterprise private sector computer security environments. The data and analysis are presented to relate lessons learned and management methodologies surrounding the principles of computer security. A benefit of this analysis was material that could augment the course entitled Secure Management of Systems by adding up-to-date information and providing real life case studies to stimulate student interest and discussion. In addition to the chapters contained within this thesis, deliverables found in several appendices include:

- Student Scenario Workbook
- Additional resources for study

The intent of the student scenario workbook deliverable is to provide a framework for Secure Management of Systems thereby restructuring the class around a single scenario and a series of related cases, all focusing on a single commercial or governmental enterprise. Presented early in the course, this scenario will provide a fundamental overview of the subject enterprise, addressing key management and employees, plant and equipment, certain affiliates, outside persons, and enterprises. Each of these is related in some significant way to the subject enterprise. The scenarios

introduce the enterprise, key managers, and certain employees to the students. Enterprise background information includes: products and/or services, locations, corporate and capital structure, marketing information, financial highlights. Employee background information includes: scholastic and job qualifications, aspects of certain employees' personal lives including financial issues, marital and other problems, etc. Individuals possess unique personalities and even quirks, to lend interest and a "real-life" look and feel to the cases. The cases highlight significant and pertinent security issues. Standard lecture will continue to be a vital part of the course. The scenario workbook can be found in Appendix B.

C. METHODOLOGY

The data collected for this work was generated using the following methods:

- Interviews: Interviews were used to get the most up-to-date, candid information.
  - Naval Postgraduate School Faculty
  - Private and Public University Faculty
  - Government Employees
  - Department of Defense Organizations
  - Private Sector Firms/Organizations
- Literary Review: This form of research allowed more in depth reading and support for topics discussed in the interviews.
  - Textbooks
  - Government Guidelines and Regulations
  - Magazine Articles
  - Books
  - Trade Journals
- NSTISSI Guidelines: These guidelines provided a framework to help choose the thesis questions.
- Internet Searches: This form of research assisted with finding news articles and additional up–to-date information.
- Other Library Resources: Additional search catalogs were consulted but these did not prove to be very useful.

The crucial portion of the research was gathered during interviews with people in the industry. A questionnaire was created based upon the primary thesis questions, secondary thesis question and several additional questions needed for supplementary information. A copy of this questionnaire can be found in Appendix C. Once the data was collected, it was then organized and analyzed. The output of this analysis was the focus of my research. To provide anonymity, the names of those interviewed and the organizations they work for are not provided in this thesis.

D. PURPOSE

The purpose of this research was to capture current lessons learned from the United States Government and private industry with respect to solving the challenges expressed in the primary and secondary thesis questions. The next step was to analyze the responses to the questions to determine the most effective answer, recommendation, or potential idea to respond to common computer security problems that are shared by both the public and private sector. The resulting analysis can be applied by other large organizations, especially the DoD. In addition, the lessons learned were formulated into case studies to be used in the teachings of Secure Management of Systems.

The first challenge was to investigate the primary questions in order to develop a good sense of the issues surrounding these questions. This was the key of the thesis: collecting good data on existing large enterprises that have each solved similar problems. Because large enterprises were the focus of the study, it was not possible to build such a system to replicate these enterprises for laboratory-like experiments and studies. Thus, there was the need to assess how existing organizations have solved security problems.

The second challenge was to organize and analyze the data and generate output in a form that conveyed the specific ideas that were found. The output needed to be presented in a concise and informative way. This particularly presented a challenge when dealing with data retrieved from personal interviews. Several interviewees would discuss tangential issues surrounding the question they were presented with. Some of this data, while interesting, was out of the scope of this thesis and needed to be excluded.

My third challenge was to marry the scenario/case model seamlessly with standard course components — slides, notes or workbook, assignments, outside readings, labs, quizzes, and exams. The proposed model affected most, if not all, of the course components to one degree or another.

I found that the data collection and analysis of real life case scenarios contributed to the development of a scenario/case model way of teaching that will be well suited to the instructional goals of Secure Management of Systems. The study of security management — including topics encompassed by the National Security Telecommunications And Information Systems Security (NSTISS) standards — closely parallels commercial and human resources disciplines successfully taught in university-level courses.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND INFORMATION

The United States Government and private industry are facing some adversity in attempting to secure their computer network infrastructure. There exists an ever-growing challenge to try and keep pace with the security issues that arise as technology changes. Large networks can exchange vast quantities of information over a global scale, and more and more people are becoming dependant on computer technology. While this is a positive tool for organizations to exchange data in this manner, it also leaves the public and private sector vulnerable to attacks by malicious users. The purpose of this research was to capture current lessons learned from Government and Industry with respect to solving particular problems associated with the secure management of large networks.

A. SECURING LARGE NETWORKS

1. Background

The DoD and other large-scale enterprises need to rely on the exchange of information in order to conquer challenges and perform day-to-day business activities. When networking came to the forefront, it provided a dynamic way to exchange information. Shared drives and email became an effective way to store and trade data. More and more information was stored in databases and on servers etc. Offices became "paperless". People started to become truly dependent on computer systems.

Access controls on information stored in these systems became critically important. While the DoD obviously held the advantage over typical large organizations with regard to physical security (part of their objective is physical security of the nation), network security was less familiar and started to become a problem. The malicious "outsiders" who were trying to gain information no longer had to physically break into a building or retain a spy inside to gain information. They merely could try and tap into the network from the outside to open up a giant world of valuable (and some not so valuable)

information. This also made the job of the malicious "insider" a bit easier. Instead of sneaking around and stealing paperwork or making copies of important documents, the insiders could now download information and email it to whomever they pleased.

2. Current State of Affairs

One can seldom open the newspaper without being able to find an article on hackers who have defaced a website or broken into a system and retrieved valuable information. The Government has taken notice of this and on October 9th, 2002 a report was generated: "*Making Federal Computers Secure: Overseeing Effective Information Security Management*" [House, 2002, pp. 1-2]. A subcommittee set up several oversight hearings to examine the following items:

- "The extent of potential threats to Government operations posed by computer viruses and worms;
- The likelihood of cyber attacks against the Nation's information infrastructure;
- The status of efforts at major executive branch departments and agencies ("the agencies") to strengthen the security of their critical computer operations and assets
- Lessons learned from the Government Information Security Reform Act of 2000; and
- The need to reauthorize and strengthen the Government Information Security Reform Act" [House, 2002, p. 2]

The "*Government Information Security Reform Act*", referenced above, was created with the intent to encourage federal entities to improve their computer security. This act provides a structure for agencies to follow, with objectives such as risk management protocols, security protocols, policy guidelines, etc. Part of the purpose of this report was to evaluate which, if any, federal agencies were following the items in the "*Government Information Security Reform Act*".

In addition to the report discussed here, the Office of Management and Budget (OMB), which is in charge of federal information security, mandated that federal agencies submit information about their computer security programs developed in

response to the "*Government Information Security Reform Act*" on an annual basis. All of this information then was incorporated in OMB's 2002 report, "*FY 2001 Report to Congress on Federal Government Information Security Reform*". This particular report isolated six weaknesses throughout the agencies that would need to be addressed, and declared the following action items:

- "greatly increase the degree of senior management attention to security;
- establish measures of performance to ensure that senior agency management can evaluate the performance of officials with security responsibilities;
- improve security education and awareness;
- fully integrate security into the capital planning and investment control process;
- ensure that contractor services are adequately secure; and
- improve agencies' ability to detect, report and share information on vulnerabilities." [House, 2002, p. 3]

The weaknesses that the committee found after its hearings were:

- "Agencies are not conducting periodic risk assessments.
- Federal computer systems have significant and pervasive weaknesses in security controls.
- Agencies do not have effective security management program controls.
- Agencies do not have effective access controls.
- Federal information technology systems rely on commercial software that is vulnerable to attack.
- Agencies' Capital Planning and Investment Control processes do not include information technology security.
- Congress does not have consistent and timely access to information it needs to fulfill its oversight responsibilities for Federal information security and related budget deliberations." [House, 2002, pp. 4-7]

Overcoming these weaknesses takes money, manpower and management support. The committee came out with several recommendations based on their findings. They are as follows.

- "The Government Information Security Reform Act of 2000 (Security Act) should be strengthened and made permanent.
- Sustained Congressional oversight is needed.
- Agency funding should be tied to the implementation of effective computer security plans and procedures.
- Congress should encourage the administration to set minimum-security standards for commercial-off-the-shelf software that is purchased by Federal agencies. [House, 2002, pp. 8-9]

Overall the findings were bleak. Agencies were given a grade from A through F as far as how well they complied with computer security standards. The report card that was generated can be found in Appendix A. The government-wide grade on this report card was an F. These findings presented information technology flaws within the Federal infrastructure. What if an attack of the magnitude of September 11th occurred in the Federal networks? This could affect the utilities, communications and emergency response infrastructures and much more depending on the nature and severity of attack.

This also brings large enterprises into the picture. Many large companies, although not related to the federal government perform services that the Government relies upon. Thus, protection of our country's infrastructure may have to extend to these large critical companies as well. There are various private entities that produce goods or services not matched by those of the Government and these companies are going to have to look at computer security seriously as well.

Large industry, although not tied down completely by Government bureaucracy, has its own problems that mirror some of the same challenges that the Federal Government is facing. Dennis Fisher, a writer for eWeek states "When it comes time to choose security products, many CIO's prefer to stick with easily understood, proven technologies such as firewalls and anti-virus software and avoid deploying more innovative systems like intrusion prevention. This mindset flows from a lack of understanding of what's required to protect a large network, as well as a sense of denial about the threats to enterprises these days." [Fisher, 2003] Fisher also points out that "The lack of interest in security can be seen in the placement of the chief security officer in most corporate organizational charts." [Fisher, 2003] The Government and private

sector are experiencing challenges in trying to press forward on the computer security front. *"The National Strategy to Secure Cyberspace"* [DoD, CIP 2003] was produced in February 2003. This document seemed to reflect the same issues brought forth in the report by the House of Representatives, *"Making Federal Computers Secure: Overseeing Effective Information Security Management"*. [House, 2002, p. 3] The purpose of this document was to "engage and empower Americans to secure the portions of cyberspace that they own, operate, control or with which they interact." [DoD, CIP 2003, p. vii] This document pointed out the close ties between government entities and the private sector in an attempt to try to improve computer security across the Nation. The report continued with, "securing cyberspace is a difficult strategic challenge that requires coordinated and focused effort from our entire society—the federal governments, the private sector, and the American people." [DoD, CIP 2003, p. vii] This thesis analyzed a set of problems that both the government and private sector share and that were focused on in the reports mentioned above. The thesis then applied these findings to support Secure Management of Systems.

B. INFORMATION ASSURANCE: SECURE MANAGEMENT OF SYSTEMS

The Naval Postgraduate School (NPS) was created by the Department of the Navy for military and associated civilian personnel to pursue higher education in order to support their career in government service. In computer science (CS), NPS specifically offers masters and doctoral degrees in computer science. There is an explicit course of study focusing on computer security, known as the "computer security track" of the CS department. This is the area in which the course Information Assurance: Secure Management of Systems is taught.

This course is one of the intermediate level courses taken by students enrolled in the computer security track. The first course is Information Assurance: Introduction to Computer Security. This course is then followed by Secure Management of Systems, which is then followed by Network Security. The course description of each of these courses is provided in Table 1.

Course Number	Course Description
Introduction to Computer Security	"Provides a comprehensive overview of the terminology, concepts, issues, policies, and technologies associated with the field of Information Assurance. It covers the notions of threats, vulnerabilities, risks and safeguards as they pertain to the desired information security properties of confidentiality, integrity, authenticity and availability for all information that is processed, stored, or transmitted in information systems." [NPS, 2003]
Secure Management of Systems	"Provides students with a secure managers view of the diverse management concerns associated with administering and operating an automated information systems facility with minimized risk. Students will examine both the technical and non-technical security issues associated with managing a computer facility, with emphasis on DoD systems and policies. Students will earn CNSS (formerly NSTISSI) certification for: INFOSEC professional, Systems Administrator, and ISSO." [NPS, 2003]
Network Security	"Addresses the concepts and technologies used to achieve confidentiality, integrity, authenticity and availability in a networked/internetworked environment. Topics include: fundamentals of TCP/IP, switching and routing, core network security principles, firewall types and methodology, packet-level traffic analysis, cryptographic protocols, virtual private networks, and public key infrastructures." [NPS, 2003]

Table 1. NPS Class Description Chart.

Together these three classes form a key part of the computer security track at the Naval Postgraduate School. The computer security track matrix of classes is also rounded out with such courses as Algorithms, Automata, Cryptography, Artificial Intelligence, Formal Methods, Vulnerability Analysis and other classes and electives.

However, computer science courses are unlike some other disciplines because it is an area that is constantly evolving. Therefore, the classes need to reflect changes in technology to make sure that students are receiving the most up to date information. Secure Management of Systems is one of those classes that teaches core issues but still will need to enhance its coursework with up to date information each quarter that it is taught.

The class is currently taught in the traditional lecture-based approach supported by a Microsoft PowerPoint slide presentation. The slides are distributed at the beginning of the quarter and students follow along and also complete the assigned reading from the chosen text. There are lab assignments and homework to be completed as well. The current outline for the class in an abstract view is as follows:

1. Security Plan

- What is it? Why have one? How do you construct a policy?
- Three Information Stages: Storage, Processing, Transmitting
- Threats, Vulnerabilities, Safeguards
- OPSEC
- Social Engineering
- Employee Awareness Training
- Project: Write a Security Plan

2. Security on the Operating System – Installation and Configuration Issues

- Tools
    - TripWire
    - Vulnerability Scanners
    - NAT
    - Imaging
- OS Configuration
    - Windows 2000/XP
    - UNIX
- CERT
- IAVA
- Mailing Lists
- Configuration Management

3 Professional Certifications

- Overview of Professional Certifications

4. Technical Protection

- Assurance Requirements
- Encryption
    - FIPS
    - NSA CCEP (Type X)
    - Key Management
        - Access, Control and Storage of COMSEC material

        - Destruction Procedures for COMSEC material
        - Identify and Inventory COMSEC material
        - Key Management Protocols
        - Report COMSEC incidents
        - Key Escrow
- Emanations
    - Shielding
    - Grounding
    - Attenuation
    - Banding
    - Filtered Power
    - Cabling
    - Zone of Control
    - TEMPEST separation
- Voice and Voice-mail Protection
- Modem Security
- Wireless Security
- Fax Security

5. Legal

- Evidence Handling
- Search & Seizure
- Entrapment
- Excessive Use
- Interviews and Interrogations
- Current Laws Regarding Information Security

6. Policies, Standards, Guidelines, and Procedures

- Overview of Policies, Standards, Guidelines and Procedures
- National Policies (OMB and NSTISSP)
- Latest DoD Policies
- Sampling of Navy, Army and Air Force policies

7. Contingency Planning

- Overview
- Data Backup
- RAID
- Hardware Redundancy
- Power Backup
- Disaster Recovery
- Forensic overview

8. Physical Security

- Computer Room Construction
- Physical Access Control
- Fire Safety
- Environmental Controls
- Alarms
- Emergency Destruction

9. Additional Items Include:

- Readings/Homework
- Projects
    - Write a Security Plan
    - Research and report on an instructor-approved task.
- Lab Assignments
    - Various Installation, vulnerability analysis and forensics

C. PROBLEM

The primary thesis questions isolated various problems in computer security and were specifically focused to gather research from large enterprises both public and private. All of these question point to an underlying theme which is moving toward an effective way to manage the security of large systems. The problem with trying to secure large systems is a problem of enormous scale with such intricate details involved that it is difficult for most entities to digest. One of the key problems with attempting to secure large systems is that the malicious user only has to find one hole to sneak into while

enterprises have to attempt to address all of the possible vulnerabilities. This can be a daunting task with the in and out flow of employees, upgrades in technology, natural disasters, malicious insiders and other challenges.

The reader should know that the attempt to secure large systems encompasses a myriad of issues not all touched on by the set of questions that were researched in this thesis. While these questions addressed some of the more contentious and difficult problems, they are not representative of all of the problems that an entity would run into while securing large systems.

It is not difficult to argue computer security is an issue in the forefront. It is hard to identify professions now that do not make use of computer systems as pointed out in "*The National Strategy To Secure Cyberspace"*.

> Our Nation's critical infrastructure consist of the physical and cyber assets of public and private institutions in several sectors: agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals, and hazardous materials, and postal and shipping. Cyberspace is the nervous system of these infrastructures—the control system of our country. Cyberspace comprises hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that make our critical infrastructures work. (DoD, CIP 2003, p. 39)

With our country's continuing dependency on computer systems, a concerted effort must be made to protect our core critical infrastructure assets. This includes protecting the systems that help to control our water supply, defense systems, transportation, communications and energy systems that include our nuclear power plants. If these systems were compromised, a myriad of possible problems could occur. Information could be leaked to foreign governments. Malicious users could take advantage of the systems to bend them to their own gain and even possibly evoking mass chaos. The list goes on.

So, how do large organizations take the necessary steps to achieve the goal of making sure that our government and large enterprise systems are indeed secure? How do they know that they are making the correct decision regarding whether to upgrade to a new system, or how to educate employees to avoid being vulnerable to social

engineering, to how to audit data and then even destroy it effectively? These questions are numerous and as soon as one is answered new technology is on the horizon to change the big picture yet again. This is similar to riding a roller coaster that may never end. Information technology managers have a challenging hill to climb and then they can glide for a while only to come upon another hill and possibly be faced with new and complex problems.

In addition, how should NPS support and teach students today about the intricacies involved in removing vulnerabilities from large-scale systems? This thesis gathered data on the eight primary questions and one secondary question posed in Chapter I: Introduction. The data gathered needed to be sorted and compressed while still retaining object lessons. This thesis then contributed the analysis of the data to Secure Management of Systems. The class itself spans one quarter – namely 12 weeks in length. This is a large amount of information to fit into one quarter. The objective here was not only to condense this information into the quarter but also to make it retainable and somewhat enjoyable for the students.

THIS PAGE INTENTIONALLY LEFT BLANK

III. PRESENTATION OF DATA

A. DATA OBTAINED FROM PERSONAL INTERVIEWS

The heart of the data for this thesis was gathered from personal interviews with employees who possess past or current experience in computer security. While there was support from articles, texts, government reports and newspapers, personal interviews remained the most effective tool for the gathering of pertinent information. What is found in an interview compared to simply reading a text on the subject is interaction with your resource. In the interview, interaction was allowed so answers could be clarified. In addition, the information was a snapshot of current affairs as compared to past information embedded in a dated report or text.

1. Personal Interview Methodology

The interview candidates encompassed all areas of the computer security area, from positions such as vice president of information technology to system administrators to computer technicians to academia. These interviews were acquired from both the public and private sector including but not limited to several branches of the military and various government agencies. Each interviewee was asked the nine original thesis questions. Additional questions were added for clarification and also to allow the interviewee to discuss their area of expertise or interest. The interview questionnaire can be viewed in Appendix C. The candidate was also asked to discuss a situation or scenario that they had experienced in their profession that provided a lesson learned. These scenarios provided an effective basis for the scenario workbook, which was a deliverable from this thesis in support of the teachings of Secure Management of Systems.

Since many of the questions asked in the interviews required that the individual expose vulnerabilities that they saw in their own organization either past or present, the large majority of the interviewees requested to remain anonymous. The data presented

below is organized to not reveal the identity of the individual and in some cases the identity of the entity to which s/he is associated. A thorough attempt was made to obtain information from reliable sources in all instances.

2. Raw Data

The following data is the raw data that was received through twenty-seven personal interviews. The following questions are the exact questions that were presented to the interviewees. (Some deviation from the question occurred according to the level of knowledge that the interviewee possessed concerning the topic of computer security.) While answers varied, there were common threads in the discussion of the questions. The data shown here is a compilation of all of the interviews meshed together. Each question will be addressed separately and the interviewee's answers will be presented with the appropriately answered questions. Bear in mind that some questions generated more discussion than others, which will be evident in the amount of raw data available. In addition, several candidates gave valuable information throughout the interview but placed constraints on what they felt should appear in writing in this thesis. As a result, some of that particular data could not be displayed but did influence some information presented in Chapter IV. Analysis of Data.

Instead of simply listing all answers, the combined answers will be shown below in the form of "response points". Several points correspond to each question. These points represent an answer or a combination of similar answers that were received while researching this thesis. Some of these points may look as if they are scattered thoughts. Please keep in mind that these points are opinions of the set of interviewees. This chapter is simply going to present the raw data. This data will then be analyzed and discussed in the next section, which is section IV. Analysis of Data.

a. Question #1 What Effect Does a Major OS Upgrade Have on the Security of a Large Enterprise?

Point 1: The difficulty of an upgrade depends on the operating system.

Point 1a: For instance, one large software vendor produces an operating system with many available features. It is a feature-driven operating system. Features introduce complexity, which then can lead to problems in upgrades.

Point 2: Some software vendors are overlooked.

Point 2a: From experience, there is a major software vendor with products that seem to have less down time, yet are still not popular due to lack of familiarity within the industry.

Point 2b: While one large software vendor beta-tests their products on the market another tend to be more reserved. The latter sends out a new operating system with tested features and a few fringe features that are usually hidden and tested by a privileged few and then tweaked as necessary. There are fewer problems when upgrading.

Point 2c. If the number of service packs out for each system is compared, there is one large software vendor that by far comes out with more service packs per operating system than does others.

Point 3: When you are upgrading an operating system you are changing an environment. Any time you change an environment there is risk. It is how you mitigate that risk that determines whether you succeed or fail.

Point 3a: In a new upgrade there are unanticipated obstacles that come into the mix. You try and anticipate all behaviors of the system yet this is almost impossible.

Point 4: Open source is a good stand-by.

Point 4a: Open source code has its merits and is usually less feature driven

Point 4b: The security risks with open source are less intense.

Point 5: When upgraded, patches and service packs must be applied in a secure and consistent manner. Sometimes even the service packs or patches themselves have bugs. The system administrator or whoever is responsible for this needs to keep on top of this situation.

Point 6: When upgrading, a combination of patches, firewalls and virus detection must be placed on the system immediately before the users get a chance to use their individual machine.

Point 7: When upgrading in a large organization you should upgrade software and hardware at the same time to avoid having to deal with incompatibility between the new software and dated hardware.

Point 8: One large software vendor shirked their moral responsibility by creating an operating system so full of holes it was just begging to be attacked.

Point 9: There are tradeoffs when performing an upgrade. These tradeoffs have to do with security, speed and money. One of these will have to suffer in order to allow the others to be successful. In other words, if you want to completely secure a system, speed may have to be sacrificed a bit.

Point 10: Application servers are coming to the forefront as being more security friendly by preventing users from installing their own software. In addition when an application needs to be updated you do not have to update it on every single machine in the organization, simply update a particular server.

Point 11: Operating system software vendors are in a tough place because security costs money and they need to make their bottom line. There are no real mandates that they build secure software. It is not a flawless business.

Point 12: Mission critical systems in the DoD are entirely different. They are virtually non-migratable as they usually have to be up and running all of the time. Therefore, there is not a great deal of downtime allowed for changes to take place within the system.

Point 13: Need to organize everything in a plan before you go into an upgrade

Point 13a: The upgrade will have to be performed at a time when it will have the least impact on the day-to-day business routine of the organization in question. In addition, an upgrade should usually be avoided during times of the year when the particular business is working to its maximum capacity. For example, you would not want to perform an upgrade at an accounting firm during tax time unless the benefits outweighed the risks

Point 14: Caution should be taken as an upgrade is performed so no malicious code is inserted at this time. The system is vulnerable at this point; one interview even referred to these as destabilizing and frightening.

Point 15: An upgrade should take place no more than once a year.

b. Question #2 Given a Large Installation of Computers, How Can Their Configuration Be Managed in a Consistent and Secure Manner?

Point 1: Disk images over a network are very effective

Point 2: A centralized server if it fits the scenario is helpful

Point 3: Roaming profiles

Point 4: Policy is very important here and needs to be set up ahead of time

Point 5: Use a proxy server

Point 6: An example to look at for the proxy server information is gotomypc.com

Point 7: Application servers are going to be the main choice of the new computing age

Point 8: If policy is in place, it needs to be clear consistent and there need to be consequences if the policy is violated

Point 9: Government currently has so many systems deployed that is had to get all of them to be able to talk to each other anyway; configuration management is virtually impossible on the older systems

c. Question #3 Given a Large Installation of Computers, How Can the Myriad of Possible Configuration Options Be Set to Support a Secure Configuration, Which Satisfies a Given Policy?

Point 1: Policy, Policy, Policy.

Point 1a: Principle of least privilege needs to be adhered to

Point 2: this depends on the operating system

Point 3: Have the employees been properly trained

Point 4: Have the system administrators been offered valuable training

Point 5: This is achievable in some situations but not all

Point 6: This is a situation where you need a buy in from the people using the system and upper management, which does not usually happen due to poor training

Point 6a: This is down at the people level and education must be mandatory

d. Question #4 Given a Large Enterprise, How Can the Large Amounts of Audit Data Be Efficiently Handled, Monitored, and Backed Up?

Point 1: Consistency

Point 2: We often collect too much that tells us too little.

Point 3: There needs to be more effective measures to collect audit data in order to be able to effectively prosecute malicious insiders. For example, look at previous breaches of information that have happened because insiders in our Government have leaked valuable information to foreign countries.

Point 4: We need a more orderly audit trail in which artificial intelligence may be incorporated to help save time when going over audit trails.

Point 5: Distributed Audit trail is desirable

Point 6: Log either side of an interface where control passes from one user to another

Point 7: This is easier today than in the past. In the past large tapes had to be used and then stored in a secure area. These took up a lot of room.

Point 8: We now have faster machines, access and forms of media that store more information in a smaller package

Point 8a: This media can be duplicated easily where before when tapes were used it took time to duplicate or if you only needed one piece you had to get to that area on the tape where now with CD's you can switch to different areas on the disk very quickly

Point 9: This is still an after the fact way to maintain data if you are using this to track people attacking your system; an IDS should be used correctly

e. Question #6 How Can Large Amounts of Data Spread Over Many Systems Be Quickly and Effectively Destroyed? (Emergency Destruction)

Point 1: If you are attempting remote destruction large magnets that could be remotely activated could help

Point 2: Microwaves

Point 3: A hammer-the old fashioned way

Point 4: Store everything encrypted and then just get rid of the key when you need to

Point 5: Thermite grenades-melts everything-used in mission critical systems-this interviewee could not expand on this subject as the rest of his information was classified

f. Question #7 How Can Large Amounts of Backup Data Be Quickly Recovered?

Point 1: Disk images are helpful so you do not have to reinstall the operating system and all of the applications.

Point 1a. Point 1 saves a great deal of time especially when dealing with numbers of computers.

Point 1b: Need to be organized as far as storage of images etc.

Point 2: The telephone companies are a good example as they have crucial systems that need to be backed up. (This tip was followed but the telephone companies did not wish to discuss their security situation)

g. Question #8 How Can Large Amounts of Data (Terabytes) Be Properly Handled in Support of Forensic and/or Prosecution Activity?

Point 1: Local police and law enforcement need to be properly trained, as they are usually first on the scene; this is getting much better.

Point 2: There needs to be specific teams to handle just this situation that are trained in forensics and the laws surrounding forensics

Point 3: The data gleaned from these activities must be logged and organized in a proper manner as things can get out of control quickly.

Point 4: State law enforcement and federal law enforcement must work together better in these situations.

Point 5: Not knowing the legal ramifications of actions while gathering this data can be devastating to lawyers as they try and build a case.

Point 6: Most organizations do not realize than when forensics becomes involved that all of their personal data can be seized by forensics and the forensics teams are not known to return this equipment in a timely manner. Companies need to have the funds or insurance to deal with this.

h. Question #9 How Can We Effectively Convey the Importance of Following Policy to Employees of a Large Enterprise to Specifically Combat Social Engineering?

Point 1: Incentive needs to be given to follow policy

Point 2: Quotes from the newspaper about computer security incidents are effective because it shows real people being impacted by malicious computer users.

Point 2a: Need to have shock value to get users to buy into the program.

Point 3: Computers have that value of "magic" where to a non-computer science major "things" just happen. Some users have a fear of computers and do not understand them so they take security risks without even knowing it.

Point 4: Encourage common sense.

Point 5: Seminars showing skits in which social engineering is used to show how easy it is to give out valuable information-effective in this particular entity when used in employee orientation. Current computer security employees in orientation put on skits about what could happen when computer security was compromised—very effective!

Point 6: Basic fundamentals need to be taught in a creative and engaging way so that they stick in the employee's head, as most employees are not going to follow an employee manual on computer security. Most employees have admitted to being too busy to read everything given to them in orientation

Point 6a: Should get to employees at orientation and then continue the education through their years of service.

Point 7: Employees simply do not see the importance unless their personal welfare has been affected in some manner.

Point 8: Military personnel respond better than civilians in these matters because they are trained to follow orders and tend to pay more attention to details.

Point 9: This entity gives tickets when they find that policy has been violated. Sticky notes are placed on your monitor. Depending on the severity of the

violation and then number of incidents, there are consequences that follow. (This is also used when for the proper handling of classified material)

i. Question #10 How Can Current Government and Private Sector Computer Security Issues Be Applied Through Case Study Analysis to the Education and Preparation of the Department of Defense Computer Security Workforce?

Point 1: More hands on experience needs to be placed in the classroom in a non-threatening manner

Point 1a: Group hands on projects usually stimulate discussion and take away the scary part of computers

Point 1b: More hands on lab time spent in a creative way

Point 2: Case studies make more of an impact than simple memorization

Point 3: Case studies (in this particular entity's training program) have provided a way to reach the employees much better than simple slides or even a basic or advanced textbook. Real life case studies provide the best source of information and provoke more questions and discussion during class time

j. Question #11 What Do You Think is the Biggest Computer Security Problem Facing the Government Today?

Point 1: Windows 2000 is a ticking time bomb and has made government facilities unsafe.

Point 2: There not only needs to be a policy but there needs to be some way to enforce policy so a laid back attitude will no longer be acceptable.

Point 3: The process needs to be simplified regarding installation of software and uninstalling software.

Point 4: The government does not understand the problem that it is trying to solve. How can you solve a problem when you cannot isolate the big issue or sub problems of the issue?

Point 5: Secure systems need to start getting more funding and research grants.

Point 6: Regular citizens need to learn about computer security.

Point 7: Computer security needs to be taken more seriously by the government.

Point 8: Programmers who are creating software need to be more concise, and aware of the security ramifications of their code.

Point 9: There needs to be better communication between the public and private sector.

k. Question #12 Are There Any Security-Based Scenarios That Have Occurred within Your Entity That You Would Like to Share with Me or Any Comments That You Would Like to Add?

This particular question asks the interviewee for any scenarios that they have run into in their past working environment. These scenarios are sometimes lengthy and full of intricate details. These scenarios are presented in Appendix B. The scenarios were compiled and some were merged together. They were then placed together in a workbook-like deliverable. These scenarios will provide support for the teachings of Secure Management of Systems.

The data presented in this section are the extra comments made by the interviewees on subjects of their choosing.

Point 1: The Government comes out with mandates or may do so in the future. They need to realize that one computer security plan does not apply to all situations. Perhaps the Government should take the approach where for example, the Government would say you need a firewall of a certain caliber and virus detection software of a certain caliber and then the entity in question could pick their own according to their needs and parameters.

Point 1a: The issues brought out by the Government need to have some teeth behind them so industry and the DoD will be forced to put a computer security plan in their budget.

Point 2: If at a minimum entities would at least do four things;

1. Patch everything and keep up with this
2. Employ the concept of least privilege
3. Use good effective passwords
4. Create a security policy that is easily explained and conveyed to employees and management

Point 3: Standardization needs to come to the forefront so that software can be measured against a benchmark.

Point 3a: The Government should have to buy off of the list of highly secure software.

Point 3b: Somehow the price of this software will have to be controlled.

Point 4: More focus should be placed on building secure software systems.

Point 5: It all comes down to the people running the systems.

Point 5a: Somehow computer security will have to become part of orientation when a new employee comes into a corporation or government agency.

Point 6: Education needs to be creative enough to get peoples attention.

Point 6a: Case studies may add the shock value that is needed to teach people what can happen if security policy is not followed.

B. DATA FROM TEXTS, INTERNET, AND GOVERNMENT REPORTS

Data was also gathered from textbooks, Internet sources, news sources and Government reports. While this data was comprehensive in nature it was difficult to obtain up to date information. Technology itself is an ever-changing area. In addition,

the structure of the Federal and State Governments were also shifting and it was challenging to get a snapshot of the current picture of how the Government was currently constructed on the computer security front.

1. Information Gathered From Text Sources Methodology

There is a great deal of information available on the topic of computer security. Research was gathered from textbooks, Internet sources and eMagazines. It was gathered from news articles and trade journals as well. Some of the information was dated. Technology changes at a rapid rate so while a history text may still reflect consistent quality information, a computer science text may not. So, some sorting of information had to occur in order to provide the most up to date view of the situation.

One challenge that was not expected but did occur was the lock down of information on DoD websites. After the events of September 11th, security measures were put into place. This included the restricting of extra information given on Federal Government websites. The reason behind the removal of this information was what is called "footprinting". "The systematic footprinting of an organization enables attackers to to create a complete profile of an organization's security posture" [Kurtz, 2001, p. 4] While this was understandable, it was sometimes difficult to obtain information concerning DoD organizations over the Internet. Private industry followed this lead and restricted some of their information as well. So, this became a challenge in this data-gathering portion of the thesis.

2. Raw Data

The following data will be presented in much the same manner as before except these points will be documented from the text, Internet source or public document in which they were found. While there is a tremendous amount of information surrounding the primary and secondary thesis questions, this thesis chose to present the most up to date information. Highlights of the data gleaned from this section's sources are shown

here. Most of the information that was researched through this type of resource was used in helping to analyze the data received in the interview portion of the research and will be seen in Chapter IV. Analysis of Data.

a. Question #1 What Effect Does a Major OS Upgrade Have on the Security of a Large Enterprise?

Point 1: "[Question]eWeek: One of the biggest complaints I always hear from private sector folks is that they don't know where to go when they find a new vulnerability or have some other problem. Will this [Department of Homeland Security] help out with that?

[Answer]Clarke: Some people in the past called the National Infrastructure Protection Center at the FBI, some people called the CERT or the FedCIRC, the federal version. The idea of putting all of these organizations together is to create a National Cybersecurity Center, which I think they will announce early next month. That center will be the obvious place to make the call." [Fisher2, 2003, p. 1]

Point 2: "SEI has also successfully developed the Operational Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), which is a self-directed approach for evaluating information security risks. OCTAVE developers published this in a book released in July of 2002 entitled: "Managing Information Security Risks – the OCTAVE Approach". More than 1000 copies of the OCTAVE Method Implementation guide have been distributed and three public training courses were offered during FY 2002. The first OCTAVE users forum was held in September 2002 in Washington D.C." [DoD, CIP, p. 39]

Point 3: The Air Force has developed the " Enterprise Network Operations Support Cell (ENOSC)" [Air Force, 2003] in order to centralize testing of new operating systems before they are deployed and upgraded in the field.

Point 4: Microsoft admitted that there was a security issue in Internet Passport, "the incident was yet another embarrassing lapse for Microsoft and could result in sanctions by the Federal trade Commission and even a staggering fine. The episode

occurs in the midst of Microsoft's "trustworthy computing initiative" to improve security for all its software products and services." [CNN, 2002, p. 1]

b. Question #2 Given a Large Installation of Computers, How Can Their Configuration Be Managed in a Consistent and Secure Manner?

Question #2 and Question #3 were both very similar. The data for both is presented together under Question #3 which is below.

c. Question #3 Given a Large Installation of Computers, How Can the Myriad of Possible Configuration Options Be Set to Support a Secure Configuration, Which Satisfies a Given Policy?

As in the first section, both of these questions, although different, still were geared to gathering similar research. The data collected for both questions is below.

Point 1: "In preventing computer attacks, Defense has to protect a vast and complex information infrastructure: currently, it has over 2.1 million computers, 10,000 local networks, and 100 long-distance networks." (GAO/AIMD-96-84, 1996, p. 4)

Point 2: "It's essential that senior management buy into and strongly support the necessity of developing security policies and an information security program.[…] Employees must be advised of the consequences for failing to comply with security policies and procedures. A set of appropriate consequences for violating the policies should be developed and widely publicized. Also, a reward program should be created for employees who demonstrate good security practices or who recognize and report a security incident. Whenever an employee is rewarded for foiling a security breach, it should be widely publicized throughout the company, for example in an article in the company newsletter." (Mitnik, 2002, pp. 261-262)

d. Question #4 Given a Large Enterprise, How Can the Large Amounts of Audit Data Be Efficiently Handled, Monitored, and Backed Up?

The information received in this area mainly consisted of definitions of concepts surrounding auditing procedures but there was a lack of information as far as how Government entities were performing audits and if so the type of software were they using. There was also a lack of information regarding which agencies were using intrusion detection systems (IDS) and if so were they using them properly and tracking their log files etc.

e. Question #6 How Can Large Amounts of Data Spread Over Many Systems Be Quickly and Effectively Destroyed? (Emergency Destruction)

There was not much information in books, Internet sources or Government reports on this topic, other than physical destruction of the equipment that contains the data and also some minor information on disk scrubbers, which are supposed to destroy the information on a hard disk at disposal time.

f. Question #7 How Can Large Amounts of Backup Data Be Quickly Recovered?

Consistency, just as in the interview section was pointed to in several areas in the textbooks. Also pointed out was the fact that media in this current day and age is much cheaper, more resilient and easier to make duplicate copies of and store. These items were pointed out across the board in texts and articles used for this thesis and noted in the reference section.

g. Question #8 How Can Large Amounts of Data (Terabytes) Be Properly Handled in Support of Forensic and/or Prosecution Activity?

Point 1: “One of the most significant challenges of investigating criminal activity in the context of pervasive computing is obtaining all of the evidence. Several

factors generally contribute to this challenge. Firstly, the distributed nature of networks results in a distribution of crime scenes and creates practical and jurisdictional problems."(Casey, 2002, p. 5)

Point 1a: "Secondly, because digital data is easily deleted or changed, it is necessary to collect and preserve it as quickly as possible. Network traffic only exists for a split second." (Casey, 2002, p. 5)

Point 2: One particular organization's paper work had a complete procedure written out in case massive system wide forensic activity was needed. This was a large company in private industry.

Point 2a: This large company had published its plan in a large thick book that held policies, plans and also had supplementary computer security teaching materials enclosed. This was geared toward their internal computer security group, which this particular company felt strongly enough to deploy.

h. Question #9 How Can We Effectively Convey the Importance of Following Policy to Employees of a Large Enterprise to Specifically Combat Social Engineering?

Point 1: "People must be trained that it is not only acceptable but expected to challenge authority when security is at stake. Information security training should include teaching people how to challenge authority in customer-friendly ways, without damaging relationships. Moreover, the expectation must be supported from the top down. If an employee is not going to be backed up for challenging people regardless of their status, the normal reaction is to stop challenging—just the opposite of what you want." [Mitnik, 2002, p. 112]

Point 2: "The moral of the story is, don't give out any personal or internal company information or identifiers to anyone, unless his or her voice is recognizable and the requestor has a need to know" [Mitnik, 2002, p. 112]

Point 3: A rather large company in private industry published a book for their computer security team. In this book was a section on creative ways to potentially

engage employees so that they could convey that there 1) was an existing security policy 2) get the employees to understand why it existed and 3) get them to feel a sense of empowerment if they followed this plan and worked with the company and not against it.

i. Question #10 How Can Current Government and private Sector Computer Security Issues Be Applied Through Case Study Analysis to the Education and Preparation of the Department of Defense Computer Security Workforce?

Point 1: "The ODUSD (S&T) oversees the Software Engineering Institute (SEI) and remain committed to train their personnel and educate them information assurance (IA) and critical infrastructure protection (CIP) awareness such that their knowledge is substantial and up to date, and to provide aggressive internal training and testing to accomplish and maintain this goal. In addition the OUSD (AT&L)-supported SEI provides staff who have designed nine training courses, to help DoD fill the number of trained professionals needed to address security issues in networked computing and increase the numbers of experts available" (DoD, CIP 2003, p. 39)

Point 1a: "SEI conducted more than 40 training sessions in the past year for technical staff, managers, and executives from the DoD, federal agencies, and industry." (DoD, CIP 2003, p. 39)

Point 1b: "SEI staff developed a training course in network security and survivability for Officers at the Marine Corps' Command and Control System school as part of their curriculum on information technology (IT) networking. This course is taught to 250-300 officers a year and has been transitioned to the Air Force." (DoD, CIP 2003, p. 40)

j. Question #11 What Do You Think Is the Biggest Computer Security Problem Facing the Government Today?

Point 1: "The Bush administration plans to appoint a new cybersecurity chief for the government inside the Homeland Security Department replacing a position once held by a special advisor to the president. Industry leaders worry the new post won't be powerful enough." (Bridis, 2003, p. 1)

Point 1a: Referring back to point 1, "'It won't work. It's not a senior enough position.' said Richard Clarke. Bush's top cyberspace advisor until he retired this year after nearly three decades with the government. Clarke's deputy, Howard Schmidt, resigned last month and accepted a job as chief information security officer for eBay Inc." [Bridis, 2003, p. 1]

Point 1b: "The new cyberchief also will be responsible for carrying out the dozens of recommendations in the administration's "National Strategy to Secure Cyberspace," a set of proposals put together under Clarke just before his departure." [Bridis, 2003, p. 1]

Point 1c: "The executives [technology executives] felt the government's plan [The National Strategy to Secure Cyberspace] was "not sufficiently strong because many of the key recommendations had been 'watered down' and were not 'mandatory'" [Bridis, 2003, p. 1].

Point 2: "The Defense Information Systems Agency (DISA) estimates that DoD is attacked about 250,000 times per year." (GAO/AIMD-96-84, 1996, p. 1)

Point 3: "DISA information shows that attacks are successful 65 percent of the time, and that number of attacks is doubling each year, as Internet use increases along with the sophistication of "hackers" and their tools." (GAO/AIMD-96-84, 1996, p. 4)

Point 4: "Currently, many of Defense's policies relating to computer attacks are outdated and inconsistent." (GAO/AIMD-96-84, 1996, p. 6)

Point 5: "The Software Engineering Institute (SEI) is host to the Computer Emergency Response Team (CERT) and the Cert Coordination Center (CERT/CC). The CERT functions include researching ways to protect information systems against potential problems, reacting to current problems, and predicting future problems. Additional duties include publishing security alerts and the handling of computer incidents and vulnerabilities.[…..] In 2002, CERT responded to over 180,000 security

incidents, handled more than 9,000 reported vulnerabilities, issued hundreds of advisories and vulnerability announcements, and coordinated with vendors in support of protecting DoD networks and responding to network security problems." (DoD, CIP 2003, p. 39)

Point 6: "The Department of Homeland Security on Friday [June 5th 2003], finally unveiled its plans for a new information security division. Although many in the security community applauded the move, they also worried that the division's as-yet-unnamed chief will be too low on the organizational chart to have much authority. […] The main objective of this division will be implementing the National Strategy to Secure Cyberspace, which has essentially been collecting dust since its release earlier this year." [Fisher, 2003, p. 1]

Point 7: Clarke also said in an interview about that the person who is chosen for the chief of cyber security that "It's very key that they get the right person; very key that person has access to the president, the homeland security advisor and homeland security secretary." [Carlson & Fisher, 2003, p. 1]

k. Question #12 Are There Any Security Based Scenarios That Have Occurred within Your Entity That You Would Like to Share with Me or Any Comments That You Would Like to Add?

As in the previous section, the scenarios found in texts, Internet sources and government reports were used to support the additional deliverable; the scenario workbook. These scenarios are lengthy and tend to involve intricate details that would be too extensive to list in this section. The scenario workbook can be seen in Appendix B.

IV. ANALYSIS OF DATA

This chapter analyzes the data presented in Chapter III. Presentation of Data. The data has been taken from personal interviews and texts, Internet sources, government reports and articles. Each of the primary questions presented in Chapter I. Introduction is analyzed here as well as the secondary question also presented in Chapter I. Introduction. This chapter will go through each question and provide an analysis that was drawn from data out of the previous chapter as well as extra information found in supplementary material.

A. PRIMARY QUESTIONS

1. What Effect Does a Major OS Upgrade Have on the Security of a Large Enterprise?

a. Operating System Upgrades

Large organizations are just that: large. That means great numbers of computers and users. A large organization can be comprised of multiple departments, sections, buildings and even be in separate states or countries. The organizations count on the flow of information in order to perform business activities. The basic element of the computer system is the hardware and software that they use. The fundamental software element is the operating system. As we have seen from Microsoft, as operating systems are placed on the market a new version is being created. This new version then comes out with desirable features. A company is then forced to upgrade because at some point the operating system is no longer supported, meaning that patches (even security patches) are no longer supplied when problems are found.

b. Affected Parties

It is the actual process of the upgrade that causes the disruption. In order to perform this function, several entities will be challenged: users, system administrators,

the system itself and management. Users will be disrupted in several ways. They will lose the use of their machine during the upgrade and they will now have to learn the idiosyncrasies of the new system. The data suggested that the best course of action for system administrators was to prepare a detailed course of action with room for unforeseen events to occur in the deployment of the new system. There is potential that they may make the decision to perform the upgrade when it will have the least amount of impact on the users. This means these employees would probably be working on holidays or late through the night putting them on an odd schedule. In addition, research suggests upgrades place the system itself in a vulnerable state. It will be in a state of change. This can be detrimental to the organization's security perimeter if not handled properly. The other factor affected here is management. Upgrades tend to run into unforeseen problems, which can disrupt users. If the users do not understand the reason for the upgrade some interviewees voiced that this can become a source of frustration as the users voice negative opinions about the upgrade process. This thereby creates tension between the IT department and the users, making the upgrade process even more difficult.

c. Type of Operating System

Several candidates gave great praise for open source operating systems. Several of them saw a migration toward open source as a good choice for the future in both the public and private sector. Price savings and security reasons were pointed out as positive reasons to upgrade over to open source. The negative reasons were said to be that a learning curve would exist. Attempting to migrate non-computer science employees who were accustomed to a Windows system to open source might be difficult and some resistance would be expected. Although, it was also noted that the open source community is attempting to become more user friendly and is also known to have more customer friendly Internet support for their products.

The attitude toward Microsoft products was mixed. Several interviewees were in favor of the software giant's products while others went as far to say that they had shirked their moral responsibility by creating an operating system so full of holes it

was just begging to be attacked. These interviewees felt that Microsoft has created an enormous market for themselves and are publicly getting pressure from all sides to move toward more secure systems as seen in this comment made after Microsoft admitted that there was a security issue in Internet Passport, "the incident was yet another embarrassing lapse for Microsoft and could result in sanctions by the Federal trade Commission and even a staggering fine. The episode occurs in the midst of Microsoft's "trustworthy computing initiative" to improve security for all its software products and services." [CNN, 2002, p. 1] However, Microsoft is a feature-driven machine. One interviewee felt that Microsoft had so many features that it made itself a tough operating system to perform upgrades on. This interview subject claimed that these features were always changing so it made them extremely hard to keep up with and that he was now favoring Apple because of the way they deploy a new operating system. Apple, he said, does not deploy a new system as often as Microsoft and tends to hold back from throwing too many features into the new mix but hides some and a certain privileged few are allowed to work with these features and report on their functionality. Whereas, Microsoft tends to beta test all features on the general public. What's more is that the number of service packs that come out for Microsoft is much higher than for open source and Apple which means that administrators of Microsoft systems need to make sure that these service packs are applied and that they themselves do not have any negative affect on the system. This just creates more work for the system administrator.

d. Risk and Mitigating Risk

One interviewee pointed out the trade-off that comes into play when making the decision to upgrade an operating system over a large number of users. One interviewee said there is a trade-off among three items:

- Speed of the system
- Money put into the system
- Security of the system

The trade-off is between these three because at least one has to suffer if the other two are desired. This is where risk and return come into play. If you have a mission critical system where safety and security are the main concern then this may mean additional features in the system that could slow it down. On the other hand, if you are dealing with a system where speed is an issue, you might need to spend more money and reduce security so as not to slow down the system. The data showed that clients both in the public and private sector are dealing with this issue. One gentleman from a space systems organization stated that they wanted all three but this was tough to achieve and there was a delicate balance among competing requirements. It seems that these trade-offs change because they are situational dependent. Yet, there was mention from a government employee that money does play a large issue in government decisions when acquiring new systems. His comments were to the effect that the government comes out with suggestions and mandates to follow for computer security but that he finds proper equipment and funds are not available to follow all of these security measures. While he acknowledged the importance of the issue, he also said that lack of trained personnel is especially detrimental when attempting to perform an operation as complex as a system upgrade. He said that training employees "on the fly" is common and not entirely ideal.

Potentially this could trace back to the government "report card" spoken of earlier in this thesis. Some agencies could not actively strive for compliance with government computer security standards because of a lack of proper equipment and manpower. This concept is supported by the data. Many government employees spoken with in the interviews stated that a lack of qualified trained personnel and a lack of funds lead to delinquencies in computer security. Private industry did not claim to have this same problem. Their problems seemed to stem more from lack of upper management support with regards to computer security.

e. Maintenance of Upgraded Operating System

As mentioned previously, each operating system has its own benefits, but maintenance of that operating system is something that must be considered when upgrading to a new system, one interviewee declared. Patches must be applied and

firewalls, virus scanners and intrusion detection systems (IDS) must be used. If an upgrade is being deployed over a large enterprise, the overhead that will come into play after the new system is intact must be taken into consideration when making the decision of which operating system to upgrade to.

f. When A Large Installation Should Upgrade

An additional supplementary question was posed: how do you know when to upgrade? The common answer was "not as soon as a new product comes out". Let others be guinea pigs for the new operating system especially if it was from a vendor with a poor history of pre-release testing. Other poor times to upgrade were when the entity was in a state of change whether it is management changes, a busy time of year, etc., or when there was a lack of sufficient funds to perform a full upgrade. One interviewee emphasized this point and then said that hardware should also be upgraded at the same time as the software to control problems arising between the software and hardware. He said that this was learned through several hard lessons and that he would strongly suggest that this as the only way to approach a major upgrade.

g. Summary

Many different approaches have been tried in order to lower the risk of problems occurring when performing an upgrade in a large enterprise. The Air Force has developed the "Enterprise Network Operations Support Cell (ENOSC)" [Air Force, 2003] in order to centralize testing of new operating systems before they are deployed and upgraded in the field. The ENOSC is responsible for being the guinea pigs before the Air Force community takes on the new systems. They are looking for bugs, problems and issues that might compromise their objective to have a smooth deployment when they perform an upgrade on existing systems. While there was some evidence that other military branches had support entities as well, the ENOSC seemed to be a highly specialized group dealing with operating systems. This might be a good entity to watch to see if their tactics are successful. If so, private industry may want to follow in these

footsteps if they have not already gone down this road. This may even generate a new form of business that could just evaluate operating systems that were new on the market and documented their problems and how to fix those problems strictly for certain clients.

Overall, operating system upgrades are complex in nature and there are many variables and trade-off situations thrown into the mix. While it seems there are strong arguments for the merits of open source operating systems, research showed that Microsoft is still the predominant choice when it comes to office software. Yet, this is the operating system that draws the most criticism.

It looks as if new ideas are being tried as far as trying to mitigate risk that a company would assume under a possible major upgrade. The Air Force ENOSC center is a prime example of this. In addition, private industry seems to be creating more and more positions within their organizations that are specific in nature to computer security.

2. Given a Large Installation of Computers, How Can Their Configuration Be Managed in a Consistent and Secure Manner?

Just as in the previous section Question #2 and Question #3 are similar in nature. The analysis for both questions will be presented below after Question #3.

3. Given a Large Installation of Computers, How Can the Myriad of Possible Configuration Options Be Set to Support a Secure Configuration, Which Satisfies a Given Policy?

Questions two and three are so similar that they will be discussed together. Configuration management is a large issue that is starting to draw more attention, as enterprises become larger and larger. Through interviews with low-level users in a particular organization, research found that they would like to have all of the software that they wanted on their own machine at work. They did not understand why they could not just download Windows Media Player or take in a CD from home and simply load software. These interviews were from a large firm where security probably should have been a priority. Both employees admitted they had installed software against the company's rules. They both admitted that they did not even know if the company had a

computer security policy concerning what they were allowed to download on their own computers. If everyone in this company decided to simply install their own software this could be a configuration nightmare.

a. Centralization

Centralization was a common answer among the interviewees. Application servers seemed to be the popular choice. With application servers, there are several advantages. One is that it is easier to set up systems for telecommuters as long as security along the hook up to the system is taken care of. It is also a way for upgrades to become more manageable. With applications installed on each users box, each box would have to be upgraded as the application needed to be. With an application server, just the information on the server has to be upgraded. This is a time saving quality for the already busy system administrator and was a popular answer within the group

b. Policy

Several interviewees mentioned policy as a "management" issue. Several times over it was said that wonderful policies were created but because there were really no consequences for violating policy, that they were not followed. This seemed to be more of an issue in the private sector where there was no type of "rank" system as in military organizations. Kevin Mitnick, who is known for his acts of social engineering against large companies has published a book which is aimed at teaching clients how to combat social engineering says this about security policy:

> It's essential that senior management buy into and strongly support the necessity of developing security policies and an information security program. […] Employees must be advised of the consequences for failing to comply with security policies and procedures. A set of appropriate consequences for violating the policies should be developed and widely publicized. Also, a reward program should be created for employees who demonstrate good security practices or who recognize and report a security incident. Whenever an employee is rewarded for foiling a security breach, it should be widely publicized throughout the company, for example in an article in the company newsletter. (Mitnik, 2002, pp. 261-262)

Several employees over a variety of industries and levels within those industries were asked about their computer security policies. The private sector seemed to show to have a large variance. Either the employee had never heard of such a computer security policy or they had not only heard of it but it was emphasized strongly in new employee orientation and consistently throughout the year. A large percentage of the public sector employees were aware that there was a policy but most of them had never actually read it personally. There were a few reports of having to read the policy and having to sign a statement stating that the employee would not be in violation of it, yet the employees interviewed said they signed so many forms upon intake into the company that they did not remember any details of the policy except to make sure they had a "long" difficult password for their own machine. Private industry where the employees had heard of the policy usually did know the highlights and basic fundamentals such as proper password use, not to bring in software from home and in addition to be on watch for social engineering. Most said that they learned this either in new employee orientation or in a supplementary brief. They also mentioned that visual aids assisted in the retention computer security concepts. One company did perform skits in order to get their point across. They had several skits that had to do with common mistakes such as poor password use, social engineering, installing software brought from home to only end up placing a Trojan horse on the system. This company said that while this was not only entertaining for the employees that they found it elevated the employee's understanding of the damage that can be inflicted by poor choices when it comes to computer security. As a result of the new employee education program, this company saw a decrease in computer security violations and improved morale and patience among the employees and system administrator staff.

c. Summary

Centralization and policy were the two main issues dealing with configuration management. Also mentioned several times was a "good plan of attack"

for how configuration was going to be handled. One organization said if configuration management is just decisions made on the fly that they believe that organization is in major trouble. They believe in a solid plan that is revised when needed.

Policy and employee buy-in to policy is also an issue. Several organizations seem to be trying new and creative ways to convey their message to new employees. It seems that the private sector is a bit ahead of the public sector in this area yet the private sector has a larger divide. Either employees have heard of a policy and are very aware of it or have never heard of it at all. The public sector employees interviewed seemed to know that a policy existed but did not know details about it.

4. Given a Large Enterprise, How Can the Large Amounts of Audit Data Be Efficiently Handled, Monitored, and Backed Up?

a. Problems with Current Auditing Systems

Audit data is kept as a record for the entity in question. This is a log of activities within the system. Almost all of the subjects interviewed mentioned the problem with auditing was too much information and not enough time or manpower to go through everything to look for a potential threat or impending attack. There were varied opinions on the value of intrusion detection systems. Some opinions were that they were an absolute necessity and there were others who said that due to lack of manpower and funds that even if they had an IDS up and running that they did not have anyone who had the time to check it in a consistent manner.

Opinions also were mixed as to whether or not IDS's based on artificial intelligence (AI) would be useful. One individual believed that a more orderly audit trail was needed and that AI would be the best way to go in order to move in this direction. He also believed that logging should take place on different sides of interfaces so that everything is logged when control passes from one user to another. This subject and others felt very strongly about audit data being handled appropriately because they believe that this is an effective tool to try to detect or track malicious insider activity.

b. Positive Issues with Auditing

Research showed that there are some positive events occurring in the world of auditing. In the past audit data had to be kept on tapes which then had to be secured in a locked room and they took up a great deal of space. In addition, one subject interviewed stated that it was more difficult to find a particular piece of data on a tape than it would be on a CD. Today, media is lighter, sometimes less expensive to buy and maintain, and more reliable. Thus, it is easier to make duplicate copies of data when needed. In addition to this, computer processing power has increased which allows faster access to data when time constraints come into play.

c. Summary

It seems that there have been several advances with physical media in the area of auditing but fewer on the software front. Audit logs are still long and tedious to review. In addition, because of all the information in the logs, it is difficult to identify anomalies in the data that could determine where an attack may be occurring. Yet, there is a push by some for an automated way to look through these files using of AI. While this push was not entirely supported by all of the subjects interviewed, there is pressure in this direction and research is being performed in this area.

5. How Can Large Amounts of Data Spread Over Many Systems Be Quickly and Effectively Destroyed? (Emergency Destruction)

a. Destruction Techniques

This proved to be an interesting question to ask. Many imaginative ideas were brought up that had to do with destroying physical media. Most of these ideas had to do with hammers, sledgehammers and other heavy-duty tools. There was one military unit that I spoke with that did use this form of destruction and had a “used equipment destruction day” but have now moved to alternative ways of doing business.

There were suggestions also of using large magnets or coils that could be placed next to the media that might need to be destroyed remotely. These magnets or

coils could be activated or heated to destroy the intended data. However, there was no information given on how the magnet or coil destruction technique would actually be implemented, or if it meets DoD requirements for degaussing. [Assistant Secretary of Defense, 2001] Space to hold these magnets and coils would also have to be considered. The question also still remains: how would they actually be activated remotely?

In addition, there was talk of using explosive devices ready to be detonated to accomplish the same task but obvious safety risks applied to this situation. There was also talk about a Thermite grenade but no more explanation could be given on this subject other than this was a device used to destroy data.

In attempting to destroy data over a large network there was only talk of encrypting data and then, when needed, destruction of the key for the encrypted data. Yet, this does not, in essence destroy the data.

b. Summary

The question regarding the destruction of data was somewhat restricted because many interviewees said that they had information on new products and services but were unable to discuss this information because it was deemed "sensitive". It seems that it depends upon whether you need to destroy data on one particular machine or data across an entire network, which then adds a bit of complexity. There is physical destruction of the data available and also physical destruction of access to the data, which are two different approaches and have different consequences. If the data were stored centrally, then it would only have to be destroyed in one place, which would make this situation a bit easier to manage.

6. How Can Large Amounts of Backup Data Be Quickly Recovered?

a. Tools

While there are several tools available that support backing up large amounts of data, the main response was regarding the consistency of the back up plan. It

was said that all the tools in the world would not help unless they are used in a consistent manner. Several interviewees talked about situations when a backup was needed only to find that the system had not been backed up for weeks and in one case, months. All agreed that consistency was key. Several military subjects mentioned that one problem they run into is the turnover rate on their employees. They have to try and bring new members up to speed quickly. This sometimes results in neglect with the back up process. This individual said he had learned his lesson and their entity now has a clear plan in place so that this will not be overlooked again, but he said this was not without suffering through many lessons learned.

One individual mentioned the advantage of using "ghosting" software. He said that his organization uses Norton Ghost for the users' machines. That way if there is some sort of malfunction in a user's computer an image is simply applied. This prevents the systems administrator from having to reinstall the operating system and all of the applications on that computer that were previously there. He did say that this does run into the entities configuration management plan and having a proper response plan in place just in case there was an emergency. If there is no plan or policy in place that dictates what to do in this situation, there may be a lack of consistency throughout the enterprise on how to effectively deal with this situation.

Another candidate used the telephone companies as an example showing the vast amounts of data that would have to be backed up in their systems. Detailed information on the telephone systems were difficult to find and all of the phone companies contacted refused to give out any information on their computer security infrastructure.

b. Summary

This question generated the least interest on the part of the subjects. As a result, the data was somewhat limited here. It seems that most individuals said that this traced back to the policy or tools that the company was able to afford to perform this job. This then goes back to the company's plan and the finances available to support that plan.

7. How Can Large Amounts of Data (Terabytes) Be Properly Handled in Support of Forensic and/or Prosecution Activity?

Forensics is a newer area in the computer security area. While the idea has been around for a while, the Government and the private sector are just starting to learn the rules and regulations regarding forensic activity and laws are just starting to appear before the United States Government on regulations governing activities to support forensics.

a. Handling Large Amounts of Data

Handling forensic activity on a single desktop is manageable but what about dealing with a large network? From the raw data we could see,

> One of the most significant challenges of investigating criminal activity in the context of pervasive computing is obtaining all of the evidence. Several factors generally contribute to this challenge. Firstly, the distributed nature of networks results in a distribution of crime scenes and creates practical and jurisdictional problems. Secondly, because digital data is easily deleted or changed, it is necessary to collect and preserve it as quickly as possible. Network traffic only exists for a split second. (Casey, 2002, p. 5)

As a network expands and grows, the forensic team has to deal with even more variables. The above quote points out that when networks for one particular entity are in different locations that this causes problems with who has legal jurisdiction over which area. The data supported that while there are better and better tools being developed everyday for forensic analysis that the real roadblock was in gathering the evidence and following the current laws on the books pertaining to this issue. The responses indicated that the legal issues surrounding forensic activity sometimes prevented the proper authorities from making aggressive moves forward in prosecution of known illegal activity. A large intricate network just inflates this problem.

The Department of Justice has even been making a move to create a team that can work between the forensic personnel and their legal side so that both can work together toward a common goal of taking care of prosecuting offenders successfully. It would be a shame if there were a known terrorist organization with obvious evidence of

terrorist activity that had been seized improperly thereby allowing the terrorists to walk free and simply set up their organization again. These are the loopholes that interviewees were gravely concerned about.

b. Suggestions for Improvement

Some of the interviewees had either been present when a forensic seizure had been taking place or had seen the after effects when one had happened. They gave several recommendations of what they thought should happen. Research showed that there needs to be some action on the part of state and local law enforcement of education of officers about the legalities surrounding the seizure of computer material. In addition, it was suggested that more forensic teams be formed, just as there are SWAT teams etc., with forensics as their specialty. Law enforcement needs to follow specific details in order to properly seize materials and this is just a larger responsibility with a larger networking environment. Logging of articles and organization are key elements for successful forensics.

In addition, companies and government facilities were not prepared for the forensic seizure ramifications when it occurred, said several interviewees. When a seizure takes place, this would mean that actual hardware could be taken from the entity in question. So, even if a company called to report some type of activity that would cause a forensics team to seize equipment there is no real protocol for return of the equipment let alone time line of when that equipment will be seen again. So, for an entity to be dependent upon their computers they would have to have the ability either survive without the equipment or purchase new equipment to take its place.

c. Secure Systems

Secure systems are an issue that is concerning some of the forensic community. While a secure operating system would be ideal for the DoD or private industry as a move toward trusted systems, this can provide a headache for the forensic teams. If these secure systems are indeed secure, it could be difficult for forensic

professionals to perform the necessary duties to pull information from computers in order to prosecute offenders. If malicious users start to use secure systems as a way to hide and encrypt their data this could work against the need to gather forensic evidence.

d. Summary

Forensic analysis faces challenges when confronted with such issues as data management over large networks, evolving legal issues, and secure systems. In the aggregate, most larger networks experience increased complexity in forensics activity than do smaller networks simply because of the larger volume of data passing through the sizeable network. As these networks evolve with changes in technology, this presents a challenge for law enforcement and the Government to keep up with the legal side of forensics. Secure systems present another obstacle. Work on secure systems could be helpful to agencies searching for a more secure way to do business but it could be detrimental to the forensic community because of the advantages and benefits that secure systems will provide to the criminal community, such as object reuse and encrypted file systems.

8. How Can We Effectively Convey the Importance of Following Policy to Employees of a Large Enterprise to Specifically Combat Social Engineering?

This question generated a great deal of discussion. Many of the comments made had to do with frustration and aggravation with upper management not supporting the IT departments of specific entities.

a. Employees

Part of this issue was already addressed in the analysis of Question #2 and Question #3. An analysis of the issue over policy will continue at this point. There was strong emphasis in the research literature showing that low-level users, who were not

educated on computer security, were not aware that a computer security policy existed within their organization. When interviewed, they also did not seem to understand why a policy would be needed.

Several candidates mentioned the word "magic" when dealing with computers. Interviews showed that low level users in both the public and private sector seemed to think that the computer processing and email, Internet etc. had some sort of magic behind it. A button is pressed and a result appears. Because of the lack of understanding of the power behind a large network, low-level users do not always understand the far-reaching effects of a breach in computer security.

Yet, some high level interviewees place this blame on higher management. They thought that it was management's responsibility to teach employees the importance of security and the consequences of their actions on the company if policy is not followed. The data showed that this is a difficult message to get through to employees. Some interviewees still showed reckless disregard whether there was knowledge of a computer security policy or not.

In the organizations where computer security education was a priority, low-level users were almost proud to explain all the rules that they learned. Research showed that organizations that placed computer security as a top priority had better retention of policies and procedures among users. In addition, organizations that made a conscious effort to be creative in conveying the need to follow policy also had good retention among users. The low-level users who had not been educated on the policy seemed to shirk answering the question and reacted almost with embarrassment that they did not know.

b. Written Policy

Another point brought up by several of the organizations making security a top priority was that when a policy is written it needs to easily readable and

understandable to a non-computer user. One particular company has a regular formal security policy and a pamphlet that it passes out as supplementary material explaining terms in the document to low level users in a creative way.

c. Summary

It seems that policy is actually a "people" issue. Any company can have a good policy but if there is not a buy-in from the employees to follow the policy then it is, in effect, non-existent.

The main consensus on both the public and private sides also is that management is responsible for this. It is the feeling that it is not the responsibility of the low level user to educate themselves on computer security but management's responsibility to convey the message in an innovative way with a goal of 100% retention across the board.

There was also mention of the consequences of not following policy. One company gives tickets on sticky notes when policy is not followed. If these tickets add up, the supervisor of the employee is contacted and an educational meeting is arranged. If the employee continues to violate the policy, then further steps will be taken. The employees in this particular program reacted positively to this and said that they also wanted make sure that they were doing their job correctly. Because what was on the other side of the tickets was predominantly education, there was a feeling among the employees that the company was not there to chastise them but almost, as one employee said, "The company feels like they let us down if we do not know the rules. Since they go to an extreme to teach us, we then feel bad on our end if we let them down. Also because we are learning, we understand why some of these rules are in place, which helps us understand the importance in following them."

B. SECONDARY AND ADDITIONAL QUESTIONS

1. How Can Current Government and Private Sector Computer Security Issues Be Applied Through Case Study Analysis to the Education and Preparation of the Department of Defense Computer Security Workforce?

This question was only asked of certain interviewees because of the nature of the question. There were several remarks made that case studies with a hands on approach would be a desirable way to teach a class.

There was a strong response by both the public and private sectors that they would like to see more hands on work in universities and colleges across the country. Some thought that case studies plus hands on work would be a good combination. Academia understood the need for slides and such, but again hands on experience was the overwhelming response by potential employers. Several subjects in the interviews supported the theoretical side of instruction in the classroom but complained that most employees lacked sufficient hands on skills that were needed to then understand how the theory could be put into practice.

Student feedback on Secure Management of Systems was gathered informally. Students did express a desire to be able to have more hands on experience through various labs that would support the course. Student feedback on having case studies in class was positive. Many said that the standard lecture format could get tedious as it is used in a large percentage of the classes at NPS. Several said the classes that they enjoy the most are the ones that touch on what is going on in the real world.

V. CONCLUSION

A. INTRODUCTION

This chapter provides conclusions and recommendations drawn from the analysis of secure systems in large-scale organizations such as those in the DoD and private industry. The benefit of this research is to provide supporting materials for the teachings of Secure Management of Systems.

B. CONCLUSIONS

The overall conclusion is that private industry and the DoD is below the standard that the Government has set a vision for. The Government in the "*National Strategy To Secure Cyber Space"* has set forth goals that they would like to achieve as a nation both in the DoD and in the private sector, but research indicates that while steps have been made toward these goals, not all of the standards are being met as seen in the research analysis in Chapter IV Analysis of Data and information presented in Chapter II Background. In Chapter II this thesis described the document, "*Making Federal Computers Secure: Overseeing Effective Information Security Management*" [House, 2002]. This document was the result of a subcommittee set up to explore the realities of what federal agencies were doing to follow federal standards relating to computer security. This is explained in more detail in Chapter II. The result was the report card shown in Appendix A. With the government-wide average being an F, it is clear that there are vulnerabilities residing in our government's computer security infrastructure.

The analysis in this thesis shows several problems within both the public and private sectors in regards to the same topics researched in "*Making Federal Computers Secure: Overseeing Effective Information Security Management*" [House, 2002]. Some of these topics are still either not being addressed or they are being addressed but are still presenting challenges to the public and private community.

There are a few major areas that were highlighted in the data and analysis found through this thesis. These were as follows:

- The attempt to secure large systems is such a complex task that it is hard to grasp on all of the problems that need to be solved in order to achieve full network security.
- There is a need for a push for continuing education in computer security at the professional level.
- Upper management will have to be convinced that there are vulnerabilities in their systems and that the effect of an attack on these systems could be devastating to our nation's infrastructure.
- Government needs to take a stronger stance when it comes to securing cyberspace.
- Government documents are being produced but there is evidence to support that their intended audience is not adhering to the suggestions set forth in these reports.
- Creative ways need to be found in order to convey the importance of policy to employees
- The *"National Strategy to Secure Cyberspace"* suggests computer security solutions but does not mandate them which leaves open the opportunity not to follow the guidelines set forth in the document.

C. RECOMMENDATIONS

Based on the conclusions mentioned above, this thesis offers the following recommendations in addition to the recommendations made in the analysis section by interviewees that participated in the research towards this thesis.

The first recommendation has to do with the media. When the United States (U.S.) first went through the AIDS scare, the media played an important role in helping to teach citizens of the U.S. the facts about AIDS. Through documentaries, news events, talk shows, interviews and movies, citizens learned how one could contract the virus, pass it along and also learned the facts surrounding the side effects of the actual virus and the medicines that were available to treat the dreaded disease. It took the media and film industry to aid in dispelling many myths that surrounded the disease.

Could this same technique be applied to computer security and have a positive effect? Could the Government step in and fund documentary research or even films to support spreading the word about the importance of computer security. The Government has nicely packaged all of their recommendations in "*The National Strategy To Secure*

Cyberspace". There is mention in this paper about how every individual, no matter how small, plays a part in securing the nation's technological infrastructure just by securing their own computers. This thesis research has shown that the average computer user is not reading this document and the need for computer security is not understood by a large portion of the population. Media might be a way to convey this message so that is reaches the nation's citizens and teaches them about security in an entertaining way.

The second recommendation has to do with the training and awareness of government employees and also private industry employees with respect to computer security policies and procedures. A central training facility for government employees might be a possibility. Creative new ways must be developed in order to find the time, space and materials to be conveyed to employees of large-scale organizations. While the data supports that many different training and awareness techniques are currently being tried such as distance learning, mandatory computer security briefs, classroom time and computer security manuals, the research is showing a lack of interest and a lack in the belief that a computer security incident could occur. There is a false sense of security that could lead to a lackadaisical attitude toward computer security. Among other things, this opens the door to effective social engineering, which leads us into the next recommendation.

The third recommendation is a continuation of the second recommendation. Social engineering is a vulnerability that was pointed out in the research by several texts and interviewees. The research suggests that a system can be using state of the art technology to lock down vulnerable areas and that all it will take is just one hole for an attacker to take advantage of. The mechanics of social engineering must be conveyed to employees of large organizations. This thesis recommends that "social engineering drills" be run in an organization just as you might run a fire drill. The computer security department could set up some potential attacks such as calling employees on the phone to try and gain password information, trashbin surfing and other sorts of social engineering tactics. When successful, they could be used (keeping the offender's names anonymous) as lessons learned. This might show employees the gravity of the situation at hand and how they themselves could be responsible for a security incident that could affect others.

Of course, a strong training program must be in place first. The employee must first be given the proper tools to combat the situation before a testing procedure would take place.

The last recommendation is twofold. Both parts of the recommendation are geared toward government creation and enforcement of computer security rules and regulations. The document, "*The National Strategy To Secure Cyberspace*" covers a large array of computer security issues. Its audience is the public and private sector and ranges from large enterprise all the way to the home users with just a single computer. However, the language that is used in this document is such that the computer security guidelines are recommendations and they are not necessarily mandated. The data suggests that there are professionals in the information assurance area who are concerned that there is not a great deal of incentive to follow these guidelines.

This first part of the last recommendation is for the government to provide some enforcement behind "*The National Strategy To Secure Cyberspace*". Take this document to the next level by possibly making it mandatory in law or add punishment for non-compliance. The groundwork is there. The data has shown that while computer security is being paid more attention to as the years progress, there is still not that sense of urgency in all communities that a breach in this security could lead to heavy consequences. If "*The National Strategy To Secure Cyberspace*" is taken to the next level, it may be possible to accelerate compliance with the goals set forth in the strategy, in both the public and private sector as well as with the home user.

The second part of the last recommendation has to do with the position of a head of cyber security in the United States Government. We have seen two people leave this post already. "'It won't work. It's not a senior enough position.' said Richard Clarke, Bush's top cyberspace advisor until he retired this year after nearly three decades with the government. Clarke's deputy, Howard Schmidt, resigned last month and accepted a job as chief information security officer for eBay Inc." [Bridis, 2003, p. 1] With two professionals retiring from the position this now leaves room for a third. The recommendation is for the government to be open to the advice of the two predecessors to this position.

The government has pushed forward and announced "The Department of Homeland Security on Friday [June 5th 2003], finally unveiled its plans for a new information security division. Although many in the security community applauded the move, they also worried that the division's as-yet-unnamed chief will be too low on the organizational chart to have much authority. […] The main objective of this division will be implementing the National Strategy to Secure Cyberspace, which has essentially been collecting dust since its release earlier this year." [Fisher, 2003, p. 1] This statement covers both points. One, that the "*National Strategy to Secure Cyberspace*" will be pushed forward and two that there will be a plan that includes the new chief of cyber security. Yet, there is still not a move to place this position higher in the chain of command. The concern is, just as it was by Richard Clarke, that the position would not have enough authority to be effective. Clarke also said in an interview about the person who is chosen for the chief of cyber security that "It's very key that they get the right person; very key that person has access to the president, the homeland security advisor and homeland security secretary." [Carlson & Fisher, 2003, p. 1] The recommendation is that the government learns from its mistakes and look to the advice of its two past cyber security advisors.

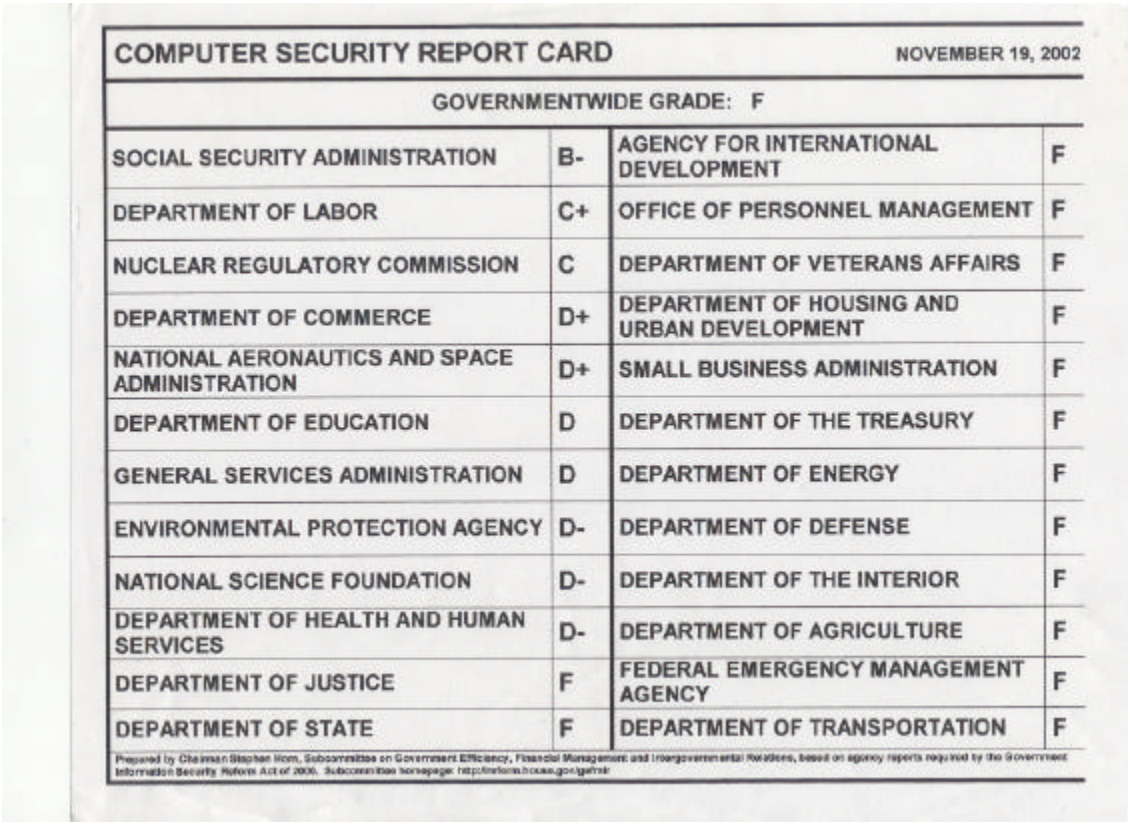
D. FURTHER RESEARCH AREAS

Further research areas that branch off the work of this thesis are:

- The structure of the Federal Government as far as reporting computer security concerns, looking for computer security assistance etc. can be confusing. An in depth look at how the Government is structured with regards to computer security responsibilities would be challenging, but productive.
- Question #1 asked about operating system upgrade issues. This question returned a wide variety of opinions and views on this subject. This question alone could fuel a compelling research project.
- The thesis research suggests that security educational tools are needed. Perhaps some interesting computer tutorials could be created to make learning easy and exciting while maintaining retention of the material as a priority. Sim Security [Thompson & Irvine, 2003] is currently being

constructed at NPS. This might provide an entertaining way for subjects to learn about computer security issues. Perhaps some exploration could be involved with students researching and writing scenarios for Sim Security.

APPENDIX A. FEDERAL REPORT CARD ON COMPUTER SECURITY



COMPUTER SECURITY REPORT CARD			NOVEMBER 19, 2002
GOVERNMENTWIDE GRADE: F			
SOCIAL SECURITY ADMINISTRATION	B-	AGENCY FOR INTERNATIONAL DEVELOPMENT	F
DEPARTMENT OF LABOR	C+	OFFICE OF PERSONNEL MANAGEMENT	F
NUCLEAR REGULATORY COMMISSION	C	DEPARTMENT OF VETERANS AFFAIRS	F
DEPARTMENT OF COMMERCE	D+	DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT	F
NATIONAL AERONAUTICS AND SPACE ADMINISTRATION	D+	SMALL BUSINESS ADMINISTRATION	F
DEPARTMENT OF EDUCATION	D	DEPARTMENT OF THE TREASURY	F
GENERAL SERVICES ADMINISTRATION	D	DEPARTMENT OF ENERGY	F
ENVIRONMENTAL PROTECTION AGENCY	D-	DEPARTMENT OF DEFENSE	F
NATIONAL SCIENCE FOUNDATION	D-	DEPARTMENT OF THE INTERIOR	F
DEPARTMENT OF HEALTH AND HUMAN SERVICES	D-	DEPARTMENT OF AGRICULTURE	F
DEPARTMENT OF JUSTICE	F	FEDERAL EMERGENCY MANAGEMENT AGENCY	F
DEPARTMENT OF STATE	F	DEPARTMENT OF TRANSPORTATION	F

Prepared by Chairman Stephen Horn, Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, based on agency reports required by the Government Information Security Reform Act of 2000. Subcommittee homepage: http://reform.house.gov/gefmir

Figure 1. Computer Security Report Card [From: House, 2002].

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. SCENARIO WORKBOOK

Scenario Workbook

The scenarios enclosed in this workbook revolve around the activities of the employees and management of the mock company Starfish Consulting Inc. This company is a large consulting firm that works with both the public and private sector. They consult in several areas such as human resources solutions, financial and budget management solutions, and technology solutions.

The company is organized in a typical hierarchical structure with a CEO, CFO and an employee tree that spreads below these positions. (There is not a top-level position that deals specifically with technology within the company).

This company resides in Largetown, North Carolina. The company is placed on the beautiful coast of North Carolina and the employees have fantastic views of the gorgeous inlet waterway from most of the available offices.

All employees access the building through two front doors. Since the company deals with sensitive data there is a key card access system imposed on these doors. There is a security guard placed at this position as well.

Scenario #1: "Give Me Some of That Beautiful Carolina Weather"

Several employees were gathered in one of the Starfish conference rooms discussing the impending hurricane threat. The local weather stated that there was a hurricane headed their way and that all safety measures should be taken when it came to dealing with what had been called "Hurricane Damon".

Starfish Consulting had resided on this coast for a while and prided themselves on being ready for these storms as this type of weather frequents the coast. They had a great deal of confidence in the structure of their building and several safety plans intact. Most of these plans had to do with evacuation of the buildings and the securing of sensitive documents etc. However, one employee, Dawn, was curious as to what happened to the servers stored in the basement of the building. She was concerned about flooding and perhaps loss of data stored on those particular servers. The Vice-President of Technology Tom, assured her that this building could stand the test of a major storm and not to worry about it.

The CEO, John, was interested in Dawn's question. After all, he was not very technically savvy and placed all of his trust in Tom's expertise. He asked Tom if they were covered in the case of an emergency situation. He asked if there was an information security plan? Tom said he would get one of his assistants to "whip one up" before the hurricane hit. John pointed out that there was a computer security users policy and did this include a protocol in it for securing data before a storm? Tom, acting a bit more aggressively this time, added that, no this was not addressed in the same brochure given out about company computer use and that one of his assistance would "get on it".

Two days later… the hurricane hit. The building did not withstand the high intensity of the wind and rain. The basement flooded. Information was lost.

1. What sort of disaster planning could this company have done in order to prevent loss of data?

2. Should employees have been briefed on the protocol for protecting the information on their systems before they left for work the day before the storm?

3. Could a distributed architecture have helped in preserving data?

4. Construct a portion of the plan that would just deal with environmental disasters that could affect the company in that area of the country?

Scenario #2: "Games people play"

Starfish was just recovering from losing the large amount of data in Hurricane Damon. It looked like their numbers were up again and they were starting to financially recover what they had lost. Sarah-a budgeting officer-was looking over some numbers for a brief to her manager on the productivity of several units in the company. She had double-checked her numbers four times but it looked like one of their units had dropped off steadily in productivity. This was a sales unit that tried to acquire new business for the company. When she looked closely at the numbers, it became clear that a certain group of employees within that unit were responsible for the drop in numbers.

Before Sarah would face her boss with this grim news she decided to visit the head of that unit. She walked down to their area and noticed that it looked as if everyone was working. Everyone was intently staring at their keyboard and typing away. Some personnel were using their phones. This group was always known to get along well and socialize after hours so it usually produced very high numbers. She could not find the unit leader so she gave up and went to her meeting.

John, the CEO, was very upset at the large drop in numbers of new business accounts. The problem appeared to be caused by the drop off in numbers usually produced by the particular sales unit that Sarah had visited. The numbers of new accounts had steadily been dropping over the last few months and were much lower than some of the less experienced sales units. John asked Sarah to check into it.

Sarah ran into one of the system administrators in the hall. He was looking upset and she asked why. He said that they needed to make improvements to the network because network traffic had been slow. One particular sales unit kept complaining that they were losing their Internet connections. He said they were almost panicked about it. I asked why and he said, online auctions of course. Sarah looked at him in amazement.

Sarah later asked the system administrator to review his audit trails. With a combination of the system administrators log files and Sarah making frequent trips to look over the shoulders of some of the employees in this unit, it became apparent that promoting sales for Starfish, was not the main priority of the day. Instead of working,

these employees had been bidding against each other for certain items on online auction sites and this had become a game that was taking up most of their workday. In addition, some were now involved in Internet gaming where they could install software on their computers to play video games against each other in the office. Sarah scheduled a meeting between Tom, Vice President of Technology, and the system administrators and suggested they discuss configuration management issues as well as policy enforcement. In the mean time she went to human resources to have them discuss information ethics with the employees.

1. What types of configuration management issues were at play here?

2. What technology solutions are available?

3. Should employee Internet use be tracked?

Scenario #3: "What is a professional?"

Tom decided to send some of his employees to a seminar on computer security to get the CEO "off his back" about the latest issues with computer security. His employees went to the seminar in sunny Florida and participated in several of the day-to-day activities. Several of the other participants at the seminar started bragging about their professional certifications, which piqued the interest of the Starfish employees. The only problem was that there were so many certifications that the Starfish employees were confused as to which ones would be the best ones for them to try and pursue when they returned to Starfish Consulting. They asked around the conference but received mixed reviews on which professional certifications they should work toward.

1. What are the different types of certifications available?

2. Why would these certifications benefit the employees of Starfish Consulting?

3. Since their jobs included trying to maintain security over a large network, what certification(s) would be best?

Scenario #4: "Spies Among Us"

Starfish consulting had one department that worked with technology consulting that did perform some testing and evaluation of code. This group worked odd hours including weekends. Ann was a programmer in this area that was consulting with a public sector entity and was working hard this particular week to finish her project. She decided that she too would "pull a weekend" to get closer to the finish line on her objectives. She noticed that Jack was in as well. Jack was another programmer who was working on a project with a telecommunications company. This was a large project and

Jack was privy to sensitive information. A lot of employees were jealous, as they believed that Jack did not necessarily deserve this position, as he was not regarded as one of the better programmers.

Ann started to notice that Jack was printing out a great deal of code throughout the day and seemed to take a lot of it home at the end of the day. She asked him why and he stated he was just doing some work at home as well.

Later that week, the manager of this section reported several sensitive documents missing from her office. When this happened again the following week, the manager reported it to the security department who, because of the proprietary status of the documents, had to report this to a federal enforcement agency.

This agency came in and set up security cameras to try and catch the perpetrator. Mock documents were placed in the security manager's office to entice the malicious employee in (if in case it was internal). Sure enough, Jack walked into the office and stole the documents right off of the desk of the manager when she was not around after normal working hours.

It turned out that Jack's father was from a foreign country and was attempting to start a large telecommunications organization. Jack's father had asked him to get any information on the infrastructure of the current telecommunications company to which he had been assigned as a Starfish consultant. Starfish prosecuted Jack for illegal activity.

1. How could this have been prevented?

2. Could access control have prevented some of this from happening?

3. If employees knew that auditing was being done, how could it have prevented this from happening?

4. Could encryption of data been helpful? How?

Scenario #5: "What is legal?"

The growing computer security problems in the technology section at Starfish were making John, the CEO, worried. He was not technically savvy but he did have an extensive business background and he knew how to identify problems and weak spots within the company.

One of the problems that he saw occurring was that his legal team seemed to be shirking their responsibilities when it came to dealing with computer security issues. They seemed confused as to the laws surrounding computer security. They were unsure how to proceed with regards to employee rights and company rights when it came to this issue. After scenario #4 occurred a law enforcement forensics team had come in and seized all of the equipment that was used in that particular section of the company. They had not been prepared for this to occur. The legal team was unsure at this time how to proceed and they were not sure what their rights were. For instance, when the forensics team came in and seized all of their equipment, the Starfish legal team did not know how

to react. They could not answer questions for John, the CEO, about how long the forensics team could keep the seized equipment, and in what shape were they mandated to return the equipment in.

John knew he needed to hire a new legal expert in this area to round out his internal legal team. This person would have to know how to deal with forensics seizures and also know how to deal with other computer security legal issues. He assigned his assistant to conduct a job search on the hunt for this new employee. He asked the assistant to meet with the Vice-President of Technology, Tom, to see what types of questions that they should be asking these candidates about their knowledge of laws regarding computer technology, specifically in the area of security.

1. What are some of the major laws in effect that this new employee should be well versed on?

2. Make up a questionnaire for this new employee so that you can see which one of the new employees interviewed would best fill the open position?

Scenario #6: "Entertaining Policy"

John, the CEO, noticed that employees were not very knowledgeable about their computer security policy. Even he did not know the main points of the security policy. He did know that Tom's new assistant, Amy, had just finalized the latest version of their computer security policy. He knew she had been working very hard on this and that she had consulted several other firms for input as to how to improve Starfish's security policy.

Amy had made the policy clearer and easier to read and had tried to make it comprehensive. She and her team had worked hard to produce a quality piece of work. John knew that Amy was the one who was the driving force behind this and suggested to Tom that her new task should be deciding how to effectively convey this information to the employees.

Tom of course had no problem delegating the work and immediately dumped the new project on Amy's desk. Amy was delighted, as she liked the human resources side of this work better than writing the actual policy. For guidance, Amy looked at what successful companies in the industry had done for training programs She found that visual aids and entertainment seemed to be key in maintaining employee interest and improving employee retention of the concepts.

Amy held a contest between several technology area teams. She gave each a topic that touched on an aspect of the computer security policy. The technology teams then were to produce a skit to show and teach other employees about this part of the policy. Prizes were going to be given for the best presentation. There seemed to be a sense of pride as the employees worked together to form their skits. The skits were presented in the company's weekly meetings and were a success. The employees had several good laughs and walked away with knowledge of the computer security policy.

This process was then repeated once a year and at new employee orientations.

1. Why do you think this was an effective way to convey information?

2. What are other effective ways that computer security policy could be conveyed with similar positive results?

Scenario #7: "Doing the right thing?"

Starfish was doing well and starting to get over some of the challenges that it was experiencing in computer security. Sales were increasing and a new section had just started in their financial division where Starfish was now consulting for high net worth clients.

Yet, John the CEO ran into another dilemma. One of these high net-worth clients was working with Starfish employee, Steve. The client had signed some documents with one of his employees, and that client had been killed in a freak accident. Steve knew that there was supposed to be a change made in a particular document and that the client was going be better off if this change was made. With the client now deceased, there was no chance that the client could come in and initialize the change. The Starfish employee-Steve-thought it over. He knew that the intentions of the client were to change the numbers in the document. He knew it was in the best interest of the client to do so. So Steve changed the numbers in the document and scanned the clients signature and applied this scan to the bottom of the new document so it looked like a copy of what the client had signed.

Because of complications that arose later, the employee confessed to what he did.

1. Could access control have played a part in controlling access to documents after a client has departed the company or in this case died?

2. What other security mechanisms might have protected the document from unauthorized modification?

3. What are the legal ramifications of this?

Scenario #8: "Final Case"

Starfish Consulting has obviously had its share of problems but now it had one more. The human resources director left the company abruptly with only two days notice. He admitted to John, the CEO, that he had joined a competitor. In addition, the director had promised two other employees, who were both system administrators, better paying positions if they left with him to join the competing firm.

Tom was worried that the three key employees, who had now left the firm, were going to share internal Starfish information with their competitor. He knew that this could have some severe consequences for Starfish, because of the amount of knowledge

that the system administrators had about the company's network. He brought a team together to brainstorm on possible vulnerabilities that could be taken advantage of by the competing firm based on the knowledge that these systems administrators had.

1. What do you think went on in this brainstorming session?

2. What types of security concerns are there when a system administrator leaves the company?

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C. THESIS QUESTIONNAIRE

Carmen Bailey
Thesis Questionnaire

This questionnaire has been reformatted to eliminate large blank areas intended for responses.

Name_____

Title_____

Specialty_____

Entity_____

Address_____

The following questions are in support of my thesis that I am currently working on at the Naval Postgraduate School in Monterey California. The title of my thesis is "The Analysis of Security Solutions in Large Enterprises". My general area of research is to analyze real world solutions to a number of security problems affecting large enterprises, such as those operated by the Navy and Department of Defense (DoD), to determine the effectiveness of each approach, as well as the commonalities and differences that approaches have when solving a particular class of problem. This thesis will then be used to support the teachings of the Naval Postgraduate School's Computer Science Secure Management of Systems (CS3670) course.

1. What effect does a major OS upgrade have on the security of a large enterprise? How can it be minimized?

2. Given a large installation of computers, how can their configuration be managed in a consistent and secure manner?

3. Given a large installation of computers, how can the myriad of possible configuration options be set to support a secure configuration which satisfies a given policy?

4. Given a large enterprise, how can the large amounts of audit data be efficiently handled, monitored and backed up?

5. How can large amounts of data spread over many systems be quickly and effectively destroyed?

6. How can large amounts of backup data be quickly recovered?

7. How can large amounts of data (Terabytes) be properly handled in support of forensic and/or prosecution activity?

8. How can we effectively convey the importance of following policy to employees of a large enterprise to specifically combat being vulnerable to social engineering?

9. How can current Government and private sector computer security issues be applied through case study analysis to the education and preparation of the Department of Defense computer security workforce? What types of tips or advice could you give me on trying to answer this question myself?

10. What do you think is the biggest computer security problem facing the government today?

11. Are there any security-based scenarios that have occurred within your entity that you would like to share with me or any comments that you would like to add/?

LIST OF REFERENCES

Assistant Secretary of Defense, Memorandum: Disposition of Unclassified DoD Computer Hard Drives, June 4, 2001.

Brenton, Chris and Hunt, Cameron, Active Defense: A Comprehensive Guide to Network Security, Sybex Inc., 2001.

Bridis, Ted, "U.S. Gov't to Get Cybersecurity Chief", The Associated Press, Washington Post, May 23, 2003.

Carlson1, Caron and Clarke, No One's Minding the Cyber Store, eWeek, April 8, 2003, [http://www.eWeek.com/print_article/o,3668,a=39889,00.asp], April 2003.

Carlson2, Caron and Fisher, Dennis, Feds to Open Cyber-Security Ops Center, eWeek, May 26, 2003, [http://www.eWeek.com/article2/0,3959,1104230,00.asp], May 2003.

Casey, Eoghan, Handbook of Computer Crime Investigation: Forensic Tools and Technology, Academic Press, 2002.

CNN, Microsoft: Flaw Left Millions at Risk, [http://cnn.technology.printthis.clickability.com/pt/cpt?action=cpt], February, 2003.

Executive Order 13010, Federal Register, Presidential Documents: Critical Infrastructure Protection, Vol. 61 No. 138, July 17, 1996.

Fisch, Eric and White, Gregory, Secure Computers and Networks: Analysis, Design, and Implementation, CRC Press LLC, 2000.

Fisher1, Dennis, DHS Unveils Cyber Security Division, eWeek, June 6, 2003, [http://www.eWeek.com/print_article?o,3668,a=43006,00.asp], June 2003.

Fisher2, Dennis, Ex-Security Czar Richard Clarke Speaks Out, eWeek, May 26, 2003, [http://www.eWeek.com/print_article/o,3668,a=42332,00.asp], May 2003.

General Accounting Office (GAO), Information Security: Computer Attacks at the Department of Defense Pose Increasing Risks, Chapter Report, GAO/AIMD-96-84, 1996.

Kurtz, George and Others, Hacking Exposed: Third Edition, The McGraw Hill Companies, 2001.

Maiwald, Eric, Network Security: A Beginner's Guide, Osborne/McGraw Hill, 2001.

Mitnick, Kevin D., The Art of Deception, Wiley Publishing, 2002.

Naval Postgraduate School (NPS), The Center for INFOSEC Studies and Research (CISR), [http://cisr.nps.navy.mil/cs3670.html], February 2003.

Office of the Assistant Secretary of Defense for the Command, Communications and Intelligence CIP Directorate, U.S. Department of Defense, FY 2002 Critical Infrastructure Protection Annual Report, 2003.

Thompson, M. F. and Irvine C. E., Teaching Objectives for Computer Security, Informing Science and Information Technology Joint Conference, Pori, Finland, 2003.

U.S. Air Force, ENOSC, [https://www.afca.scott.af.mil/osc/contact_us.htm], February 2003.

U.S. House of Representatives, Making Federal Computers Secure: Overseeing Effective Information Security Management, U.S. Government Printing Office, Washington D.C. 2002.

The White House, The National Strategy to Secure Cyberspace, [http://www.whitehouse.gov/pcipb/], February 2003.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Dr. Ernest McDuffie
   National Science Foundation
   Arlington, Virginia

4. RADM Zelebor
   N6/Deputy DON CIO
   Arlington, Virginia

5. Russell Jones
   N641
   Arlington, Virginia

6. David Wirth
   N641
   Arlington, Virginia

7. CAPT Sheila McCoy
   Headquarters U.S. Navy
   Arlington, Virginia

8. CAPT Robert Zellmann
   CNO Staff N614
   Arlington, Virginia

9. Dr. Ralph Wachter
   ONR
   Arlington, Virginia

10. Dr. Frank Deckelman
    ONR
    Arlington, Virginia

11. Richard Hale
DISA
Falls Church, Virginia

12. George Bieber
OSD
Washington, D.C.

13. Deborah Cooper
DC Associates, LLC
Roslyn, Virginia

14. David Ladd
Microsoft Corporation
Redmond, Washington

15. Marshall Potter
Federal Aviation Administration
Washington, D.C.

16. Ernest Lucier
Federal Aviation Administration
Washington, D.C.

17. Keith Schwalm
DHS
Washington, D.C.

18. RADM Joseph Burns
Fort George Meade, Maryland

19. Howard Andrews
CFFC
Norfolk, Virginia

20. Steve LaFountain
NSA
Fort Meade, Maryland

21. Penny Lehtola
NSA
Fort Meade, Maryland

22. Paul C. Clark
Naval Postgraduate School
Monterey, California

23. Dr. Cynthia E. Irvine
Naval Postgraduate School
Monterey, California

24. Carmen Bailey
Naval Postgraduate School
Monterey, California