AFIT/GIR/LAS/99D-5

INFORMATION SYSTEM INCIDENTS: THE DEVELOPMENT OF A DAMAGE ASSESSMENT MODEL

THESIS

Mark D. Horony, Captain, USAF

AFIT/GIR/LAS/99D-5

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the US Government.

AFIT/GIR/LAS/99D-5

INFORMATION SYSTEM INCIDENTS: THE DEVELOPMENT OF A DAMAGE ASSESSMENT MODEL

THESIS

Presented to the Faculty of the Graduate School of Engineering and Management

of the Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the Degree of Masters of Science in Information Resources Management

Mark D. Horony, B.S.

Captain, USAF

December 1999

Acknowledgements

I wold like to express my thanks and appreciation to my advisor Maj Dave Biros. His guidance and support provided a strong foundation for me to complete this thesis. His knowledge and expertise in information warfare and assurance established a basis for me to build my research. In addition, I would like to thank my reader, Dr. Guy Shane for his contributions to the structure and analysis of the data collected. I am also indebted to Dr. Heminger for stepping in as an additional reader and providing guidance and support following the closure of the School of Logistics and Acquisition Management and the departure of Dr. Shane.

I would also like to say a special thank you to all the senior level information managers who sacrificed their valuable time to become a subject in my thesis. Without their background knowledge in the area of information security and management, this thesis would not be possible. In addition, I would like to say a special thanks to the "Sweat Hogs" for working late too and their support and encouragement during those final hours.

Most importantly, I would like to thank my wife, Staci and children, Jessica, Zachary, and Ryan whose support and sacrifices allowed me to dedicate my efforts to this thesis and graduate program. Without their sacrifices, I could not have completed this program. Staci, thank you from the bottom of my heart.

Mark D. Horony

Table of Contents

Page

Table of Figures

Table of Tables

Abstract

Information system (IS) incidents, such as hacking, denial-of-service, and viruses are on the rise. With low manning and under-trained information security specialists it is difficult for organizations to stop IS incidents from occurring. Once an incident has occurred it is the IS manager's responsibility to ensure that a full and accurate damage assessment has been accomplished. However, most IS managers lack the necessary tools to assess the damage from an incident.

This exploratory thesis developed an IS incident damage assessment model (DAM) that can be part of the IS manager's tool kit. During the development of the model, it became apparent that everything in the model was supported by a foundation of business processes. Therefore, the most important thing an IS manager can do is define their organization's business processes and how they relate to information systems. The model is based on eight primary factors that should be considered during the assessment process:

- Recovery
- Education/Training
- Business Expenses
- Productivity
- Data
- Lost Revenue
- Reputation
- Human Life

Each factor is then further expanded into sub-factors that better define and explain the primary factors. These sub-factors can be directly mapped to business processes previously defined by the information system manager. The final product is an IS incident DAM tailored to the needs of the IS manager's organization.

This page left blank

INFORMATION SYSTEM INCIDENTS:

THE DEVELOPMENT OF A DAMAGE ASSESSMENT MODEL

I. Introduction

> Since everything, then, is cause and effect, dependent and supporting, mediate and immediate, and all is held together by a natural though imperceptible chain which binds together things most distant and most different, I hold it equally impossible to know the parts without knowing the whole and to know the whole without knowing the parts in detail.
>
> Blaise Pascal

Overview

The Computer Emergency Response Team (CERT), at Carnegie Mellon University's Software Engineering Institute was established in 1988 and received only six information system (IS) incident reports their first year. Incidents include such things as hacker attacks, denial-of-service, and viruses. Ten years later, in 1998, they received 3,274 information system incidents reported and the reports for the first three-quarters of 1999 had skyrocketed to over 6,800 (CERT®/CC, 1999a). This is only one example of the growing number of problems information security specialists must confront on a daily basis. The information they must protect is an extremely valuable resource that, when used properly, can persuade and manipulate people and countries. Today more than ever, the rapid growth of the Internet and its related intranets and extranets illustrate the importance organizations and people place on sharing information. Each day businesses, governments, and individuals transmit billions of bytes

of information and data over the Internet (CERT®/CC, 1999a). The information transmitted is such a valuable and vulnerable commodity that individuals and organizations will attempt to steal, destroy, or manipulate it inflicting damage to the owner of the information (Vatis, 1999; Willemse and du Toit, 1996). Once the information has been damaged it becomes a complicated and enormous task to assess the details of the damaged to the parts or to the organization as a whole (Amoroso, 1999).

The birth of the Internet in the late 60's produced a new type of criminal, the cyber criminal. Cyber criminals use creativity, knowledge, software, and hardware to attack and infiltrate information systems (IS) in order to copy, delete, or manipulate information. The cyber criminal is seeking information such as credit card numbers, government documents, and bank account numbers stored at various Internet sites around the world (Denning, 1999). In the beginning, the cyber criminal's activities were mostly limited to accessing and obtaining information stored on university and military computers (Denning, 1999). As the number of businesses and military installations connected to the Internet grew the amount and variety of stored information available to the cyber criminal grew. The increased volume of information available on the Internet led to an increase in cyber criminals and a variety or cyber crimes such as attacks, intrusions, introduction of viruses, and data theft to mention a few.

The increased availability of information was only one factor, another factor was the increased availability and sophistication of hacking tools and software programs (Pethai, 1996). In the beginning, these tools were nothing more than hackers using modems, attempting to gain access by guessing passwords. As technology progressed hackers began developing and

sharing automated tools to guess passwords, dial telephone numbers, crack passwords, and more (Hafner and Markoff, 1992). Over the years these hacking tools have become even more specialized, more sophisticated, and more available, thus reducing the knowledge, skills, and expertise required to successfully attack and gain access to an information system (McCune, 1998; GAO/ T-AIMD-96-108, 1996). The Internet has made these automated tools readily available to anybody to download and use at their convenience (Kammer, 1999). An example of how easy it is to obtain a set of hacking tools is the use of Internet search engines. Using the search engines and the terms *hacking tools* and *hacking software* returned over 20,000 instances of hacking tools listed on the Internet. Figure 1 shows that as the sophistication of the hacking tools has increased over the years the knowledge required to successfully intrude on a system has dropped (Didio, 1998).

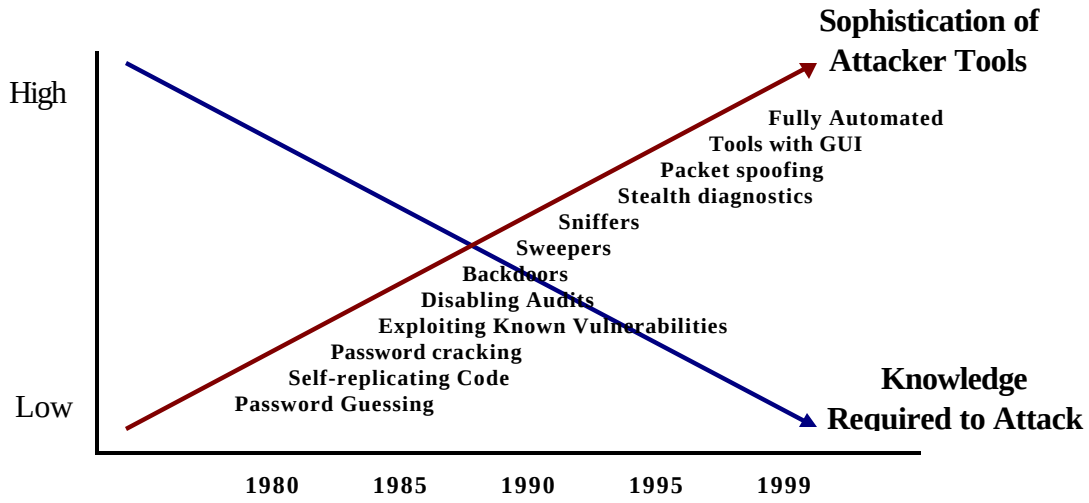

Figure 1: Attacker's Knowledge and Tools (Didio, 1998)

Problem

As hacking tools become more sophisticated and the number of incidents increase organizations using information technology are targeted by cyber criminal. Regardless of the type or duration of an information system incident there will be some damage to the system and organization (Denning, 1999). Current methods for damage assessments are unstructured, ad hoc, and narrowly focused only on system damage (FBI, 1999, Hamilton, 99). There is no continuity among industries and information system managers to perform damage assessments of IS incidents. Additionally, the literature covering damage assessments is anecdotal in nature and lacks explanations of methods used by organizations to assess the true damages caused by intruders and incidents (FBI, 1999). When an information system incident does occur, what factors should be considered by IS managers to conduct a damage assessment? The objective of this thesis is to collect data from information system managers and develop an information system incident damage assessment model (DAM) to be used following an incident.

Summary

The growth of the Internet and its related intranets and extranets along with the proliferation of information stored by public and private organizations on information systems is contributing to the increased number of cyber criminals. Additionally, the growing sophistication and availability of automated software hacking tools is making it easier for a computer novice to become a computer criminal. As the number of incidents increases the need to assess the damage caused by these incidents is also increasing. This thesis will use upper-level IS

managers to help determine what factors needs to be addressed when performing an IS damage assessment. This information will be used to develop a DAM.

Chapter 2 will cover the current research and information available in the area of damage assessment models and information system intrusions. Following this, Chapter 3 will be an explanation of what method will be used to collect the data. Chapter 4 will cover the data analysis and results from the data collection. The findings and their relevance to the problem will be discussed in Chapter 5. Additionally, Chapter 5 will present some limitations of the study with recommendations for future research.

II. Literature Review

Introduction

The amount of literature found that discusses the use or construction of standard models or methods for conducting information system damage assessments was limited. Research and studies covered related topics such as increased cost of computer intrusions (no methods for costing), increased number of intrusions (Vatis, 1998), the legal problems of intrusions (Greenwald, 1997), and IS security issues (McCune, 1998). This chapter will discuss how increased application of information technology and expansion of the Internet has contributed to a rising rate of information intrusion. In addition, it will cover training issues relating to information security, legal issues relating to information system incidents, and the current state of research relating to damage assessment models and methods.

Increased Use of Information Technology

Organizations have increased their use of information systems over the past 20 years and their IS budgets are still on the rise (Martell, 1997; Schwartz, 1999). Worldwide spending on technology in the high-tech industries is expected to increase from $950 billion in 1996 to over $1.4 trillion by 2000 (Electronic News, 1997). Organizations are increasing their IS budgets to add advanced technologies such as mobile computing, remote connectivity, and virtual private networks to their business infrastructure (Mosquera, 1999) in hopes of increasing their profit and productivity (Brynjolfsson and Hitt, 1999). One very popular and widely used technology is the Internet and businesses are embracing its potential for profit by establishing a

presence, or storefront, on the Internet to conduct business (Dalton, 1999; Mosquera, 1999). However, every connection an organization has to the Internet is a door that must be protected and secured from potential cyber thieves and criminals (Vatis, 1999). These doors increase the threat of information system attacks (Mosquera, 1999; FBI, 1999).

In spite of the increased threat to organizations, businesses are flocking to the Internet and electronic commerce in record numbers (Colkin, 1999; Dalton, 1999; Shulman, 1999). In 1998 Shop.Org, a consortium of over 200 online retailers, contracted Boston Consulting Group (BCG) to conduct a survey to determine the expected growth of online retailing and to set benchmarks for continued monitoring of the statistics. BCG's 1999 survey showed a 200% increase in online retail transactions for 1998. In addition they expect 1999 online revenue to exceed $36 billion, this represents a 250% increase from the 1998 revenue (Boston Consulting Group Report, 1999). With this potential for revenue and the number of businesses using the Internet, it seems that the end to the growth of electronic commerce is nowhere in sight. The growth of electronic commerce is mutually beneficial to the business and the consumer. As more consumers use the Internet they begin purchasing products offered on the Internet (Colkin, 1999; GVU, 1999). The annual increases in revenue from Internet purchases encourages more retailers to develop an electronic commerce presence on the Internet (Triendle, 1999). The increased number of retailers provides a larger variety and quantity of products available over the Internet, thereby drawing more consumers online to purchase the ever increasing variety and quantity of products, thus completing a circle (Dyson, 1997). Though this expansion of the Internet and electronic commerce is a benefit to the consumer and businesses, it becomes a

problem for the information security managers by increasing the likelihood of information system incidents (Vatis, 1999).

Lack of Training

Fueled by the increased use of information technology in businesses there has been a rapid and significant expansion in the information technology industry over the past two decades. With businesses adding information technology to their infrastructure, information managers need qualified and trained people to protect and manage the new systems. The demand for workers in the information technology career field is so great that the Bureau of Labor and Statistics (1999) has classified computer related careers as the fastest growing job market and predicts it will remain this way until 2006. The sudden growth of information technology has produced a vacuum of qualified workers to support the expanding infrastructure (BLS, 1999).

One critical job among the IT support personnel is information security. Information security managers and technicians are a critical resource needed to protect the various pieces of business IT infrastructure (Kammer, 1999). The large demand and inadequate supply of information technology workers, specifically information security managers and technicians, often forces organizations to hire under-qualified and under trained personnel (Technology, 1999; Wright, 1997). Regardless of whether information security personnel are qualified or unqualified, it is difficult to find time to train and remain proficient in security issues with the rapid changes in information technology, software, and the release of new hacking tools (Vatis, 1998). The National Institute of Standards and Technology estimates that about 30 new

hacking tools are developed and posted to the Internet every month (Kammer, 1999). To stay current, information security personnel must constantly receive new training, while at the same time ensure their business infrastructures are safe. They are relentlessly trying to find ways to detect and neutralize the new and sophisticated tools cyber criminals employ in order to protect the business information systems. The training they require can be accomplished through on-the-job-training or training programs taught internally or externally to the organization (Technology, 1999).

One advantage of on-the-job training and internal training programs is it provides the business with a more controlled and organizationally focused training program (Hamilton, 99). In addition, the business can tailor the schedule of the information security manager or technician to meet the needs of the organization. A disadvantage of this type of training lies in the rapidly changing field of information technology (Vatis, 1999). It is expensive and time consuming to establish and maintain an internal training program (Internet Engineering Task Force, 1997). Training instructors must constantly modify the material to meet the needs of the rapidly changing information security field (Internet Engineering Task Force, 1997). In order to reduce the cost of internal training programs increasingly organizations are leaning towards external information security training. External training programs normally have the resources to remain current and provide quality training. However, it is expensive and time consuming with classes often exceeding a week in duration. During the external training, the organization loses the employee for the duration of the training class, normally leaving the organization understaffed.

Information management is another area lacking appropriate training in information security (Wright, 1997). Wright states that universities fail to adequately educate managers and information managers in the field of information security and goes on to say "In order to improve the existing state of computer and network security, INFOSEC [information security] education must be integrated into the curricula of colleges and universities" (Wright, 1997: 17). Western Connecticut State University did exactly that; they established an Information Security Management degree program in their school of Business with the goal of teaching managers better information security skills (Wright, 1997). Without the proper training and education to manage information security, it is difficult to investigate the rising rate of computer crimes.

Even with the best training and education, information security managers can not stop every intrusions (Ruben, Geer and Ranum, 1997). When an intrusion does occur and an unauthorized user gains access to an information system it is difficult for information security personnel to conduct a damage assessment without the proper knowledge, skills, and training (Kammer, 1999). An information security survey conducted by InformationWeek/Ernst & Young reported that 70 percent of the companies and organizations surveyed, incurred a loss as a result of an intrusion and lacked the knowledge or skills necessary to accomplish a damage assessment (Violino, 1996: 68-69). It is importance to conduct a damage assessment so system administrators have the necessary information to recover and rebuild the system (Toigo, 1996), management can establish and justify information system security budgets, and for litigation is established should the organization decide to take the incident to court.

Increased Information System Incidents

The increased use of advanced information technology by business, the ever-expanding information technology career field, and the lack of trained and experienced information security personnel all contribute to an ever-increasing modern problem, computer crime. Computer crime and information system intrusions are on the rise (CERT®/CC, 1999; Rutrell, 1998; Howard, 1997). Figure 2 shows that, except for a dip in 1997, the number of information system incidents reported to the CERT have been steadily increasing reaching an apex of over 6800 incidents in the first three quarters of 1999 (CERT®/CC, 1999a). The CERT (1999b) defines an attack as a single attempt to gain unauthorized access to a site and an incident as several attacks, possibly by several

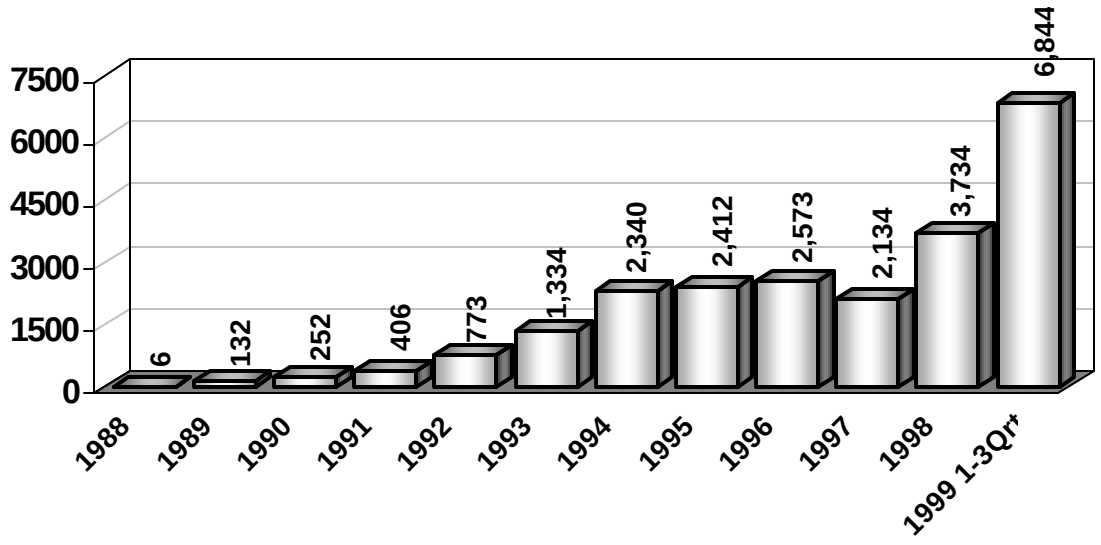

Figure 2: CERT®/CC Incidents Handled

individuals working together. The CERT's statistics only represent the incidents reported to the CERT and many organizations do not report IS incidents in fear of negative publicity

(CERT®/CC, 1999a). This is a possible indication that the actual number of incidents is much higher then number reported by CERT.

Similarly, an FBI and Computer Security Institute computer crime survey conducted over the past 4 years shows some interesting trends in computer incidents. The 1996 survey showed that 42 percent of companies surveyed said they had incidents of unauthorized use of their computer systems. By 1999 the incident rate of surveyed organizations had risen to 62 percent (FBI, 1999). The same FBI (1999) survey showed the percentage of organizations surveyed that reported incidents to law enforcement doubled from 16 percent in 1996 to 32 percent in 1999. The increased reporting of incidents to law enforcement may be an indicator that organizations are beginning to realize the damage being caused and are trying to do something about it.

Legal Need for Damage Assessments

Over the past two years, the FBI's National Infrastructure Protection Center's (NIPC), established by executive order in 1998, caseload of computer crimes has increased by 200% (Vatis, 1998). However, it is not certain whether the increased caseload is from an increase in computer attacks or the fact that more organizations are involving law enforcement by reporting computer crimes. The FBI is not the only law enforcement agency affected by the increase in computer crime. Other police departments in the United States are creating high tech crime squads to investigate and catch would be computer criminals (Vatis, 1998).

When these law enforcement agencies take a computer crime to court, it is important they have the facts supporting their case. According to current federal civil and criminal law,

§1080 Computer Crime Statute, crimes involving computers require the substantiation that the plaintiff has incurred damage. The reason for this substantiation is the punishment of an offense is based on the amount of damage caused by the defendant (Kratz, 1996). Therefore, to assist law enforcement, it is important that information security managers be able to accurately and consistently conduct damage assessments of information systems incidents and be able to attach a value to the damage. Sterling (1992) gives several examples of how the lack of good evidence and damage assessments lead to individuals accused of the computer crimes being acquitted. A standard model for damage assessment could help information managers produce reliable damage assessments for litigation purposes.

Lack of Damage Assessment Models

Professional and academic journals cover topics such as information system security, managing security, managing information systems, and costs related to creating and managing information systems. However, the literature review supporting this research could find no reference to damage assessment methods or models. Likewise, the professional organizations such as the CERT®/CC, Forum of Incidence Response and Security Teams (FIRST), and AF Computer Emergency Response Team (AFCERT), responsible for incident handling provide limited guidance on damage assessments.

Journals. Searches through professional and scholarly journals resulted in no research trying to categorize or establish a standard method for conducting damage assessments of information system intrusions. There were no results discussing standardized methods or models for damage assessments when using an Internet search engines and terms such as

damage, *assessment*, *information security*, *intrusions*, *risk analysis*, and *disaster planning*. During the course of the research, the information found in journals and on the Internet relating to the subject of information system incidents and intrusions fell into three categories: security (or prevention), detection, and recovery.

Information security is a source of very active debate (Anderson, 1998) and a growing market (Ott, 1999) in the information technology industry and business world. The information security industry is a billion-dollar a year industry and is expanding every year (Trigaux, 1996). According to a Computer Security Institute (CSI) study, over 60 percent of surveyed companies plan to increase their information security budget during 1999 (ComputerWorld, 1998). A reason for the growing information security budget is the need for organizations to protect their increasing IT infrastructure (Vitas, 1998). Prevention methods employed by information security personnel include everything from firewalls to anti-theft devices for personal computers. Often information system security is not enough (Denning, 1999).

In recent years, many universities and software developers have begun developing intrusion detection systems (IDS) to help combat the rising rate of computer intrusions from both inside and outside of an organization (CERIAS, 1999; FBI, 1999). The Center for Education and Research in Information Assurance and Security (CERIAS) at Purdue University, was established to "advance the philosophy of information security and assurance" (CERIAS, 1999). One way CERIAS accomplishes this goal is through being a central point of research information between commercial, government, and academic institutions. One of their major projects is organizing, guiding, and encouraging the development of better IDS (CERIAS,

1999). Nevertheless, sometimes even the most sophisticated information security systems, firewalls, and intrusion detection systems can not prevent intruders (Anderson, 1998).

In the event that an information system intrusion does occur, a disaster recovery plan is a manager's way to mitigate the risk of serious or catastrophic loss (Toigo, 1996). The field of disaster recovery planning is starting to take a more serious look at the recovery of information and information systems following a natural disaster. However, disaster recovery planning focuses on physical damages and loss due to natural disasters and not on the damage assessment issues relating to costing a disaster (Technology, 1999; Toigo, 1996). Organizations that implement disaster recovery plans focus on getting systems up and running as quickly as possible (Toigo, 1996). This may be because research has shown that the average acceptable downtime, before the loss of business functions become unrecoverable is 72 hours (Toigo, 1996). This means that in order for a business to survive a disaster it is important that they have a tested and working disaster recovery plan in place. Even though managers rate a disaster recovery plan as a critical need, research in this area suggests that organizations fail to test their disaster recovery plan often enough to ensure it meets the organization's needs and that the plan works as expected (Straub, 1998;Technology, 1999). Research in the area of disaster recovery planning lacks the discussion damage assessments models for information systems incidents.

Computer Emergency Response Teams. Following a major Internet virus incident in 1988, the Advanced Research Projects Agency (ARPA) created the Computer Emergency Response Team/Coordination Center (CERT) at Carnegie Mellon's Software Engineering

Institute to track and control incidents occurring on the Internet (Harvey, 1991). The CERT became a clearinghouse for information related to network computer vulnerabilities and intrusion attempts. Private and public organizations regularly report incidents to the CERT. The emergency response teams (ERT) primary focus is to collect data related to computer incidents, develop corrective actions, and disseminate this information back out to the information system managers (CERT®/CC, 1999b; AFCERT, 1999). They are a clearinghouse for information security issues and provide services such as incident tracking and monitoring, virus notices, security information database, and system recovery procedures (CERT®/CC, 1999b, AFCERT, 1999). The ERTs do not concern themselves with damage assessments beyond the information needed to recover from an incident. Their damage assessments do not include methods or models that try to determine the impact of an incident on the business. The CERT publishes a handbook for system recovery, following an intrusion, and it mentions costing the incident as a procedure to follow during recovery; however, they provide no guidance or direction on how to accomplish the task (CERT®/CC, 1999b). Similarly, the Internet Engineering Task Force (IETF) created a Site Security Handbook that extensively covers system recovery following an incident, yet only mentions "assessing the impact" without any further guidance or direction on how to accomplish the task (IETF, 1997). Overall, the ERTs provide limited direction to organizations on how to assess damages and even less information on what to assess following an incident.

Available Research in Damage Assessment. This literature review found a very limited amount of research on DAMs relating to information system incidents. One research report that

is available on assessing incidents is a study conducted by Rezmierski at the University of Michigan. Rezmierski (1998) conducted the study on behalf of a request by the Chief Information Officers of the Committee for Institutional Cooperation (CIC), a consortium of the Big Ten universities and the University of Chicago. The scope of the study was limited to academic organizations and included physical losses, such as theft and vandalism, and system intrusions (Rezmierski, 1998). One observation made by Rezmierski (1998) in the study was that organizations actively avoided the negative publicity associated with IS problems and intrusions by not reporting incidents to law enforcement or news media. Many researchers agree that this is a primary reason that research into costing IS incidents is so difficult and why historical data about intrusions are not available (Straub, 1998; FBI/CSI, 1999; Hamilton, 1998; Rubin, Geer and Ranum, 1997). Rezmierski's (1998) study also found that incidents relating to information systems are divided into two primary categories: quantifiable and unquantifiable costs. These can be referred to as tangible and intangible, respectively.

Tangible Costs. Tangible costs are less difficult to determine and are considered objective in nature. According to Rezmierski (1998), risk managers and auditors often describe tangible costs as direct costs that typically result in direct payments of some kind. These costs can include such things as man-hours to recover or rebuild the system, employee down time due to system outage, and new software purchased to recover or protect the system.

Intangible Costs. Rezmierski's (1998) study states that the intangible costs "have the potential to be of greater magnitude than the direct effects and result in much greater total cost" and are often ignored by risk analysis managers, auditors, and information security managers

(Rezmierski, 1998). They will focus on the tangible costs that are easier to count and quantify. The intangible cost include things like the reputation of an organization, lost business due to loss of reputation, lost confidence, and even legal liabilities (Rezmierski, 1998). Greenwald (1999) discusses some legal liabilities and how rapidly insurance companies have to change their methods for insuring Internet based businesses. Information technology has created new legal issues such as the value of information, confidentiality of data transmissions, and ownership of information that insurers have not had to deal with until recently (Greenwald, 1999). Many of these issues can be considered intangible in nature and very difficult to assess.

Current Methods. Magazine and newspapers are constantly publishing reports of damages and costs of information incidents. They report instances such as "Computer Crime Costs Britain $1.5 billion a Year,"(1996) or "Firms Say Hacker Cost Them $291 Million,"(CNNews, 1999). A FBI (1999) computer crime survey shows, of the organizations surveyed, that financial losses rose from $100.1 million in 1997 to over $123.8 million in 1999. However, none of the sources explained a method for determining the losses. Actually, the same CNNews report that claimed $291 million in losses also mentions the large ambiguity in estimating costs relating to information incidents (CNNews, 1999). In addition, the FBI (1999) computer crime survey says that 51 percent of the companies surveyed reported financial losses, yet only 31 percent of the surveyed companies reported they could actually quantify the loss. The editor of the FBI survey, (FBI, 1999) stated that even the FBI computer crime survey is unscientific in nature and the figures are only a rough estimation of true losses. Currently the primary method for calculation of financial loses is to calculate the man-hours

needed to recover from an incident (FBI, 1999; Toiga, 1996). This includes items such as the time spent to rebuild a system, time to restore data lost, time to re-enter lost data, and time spent on investigating the incident. These calculations focus on the system recovery and ignore the potential damage an information system incident may inflict upon the business processes of an organization.

Summary

The use of information technology is on the rise and with it the number of computer crimes and intrusions. The information security industry can not keep pace with either the demand for skilled workers or protection of organizational IT infrastructure. Because of the high demand and shortage of workers in the information technology career field, the workers hired as information security technicians and managers are often under-qualified and lack the necessary training and skills to protect the information systems. Without trained and skilled information managers to provide an accurate damage assessment, litigation is difficult and prosecution is even harder. The available research in damage assessment is insufficient to establish an accurate and standard model or method to support information managers in performing a damage assessment. The only study found that specifically addresses damage assessments is the costing study conducted by Rezmierski for the CIC. Current methods are not sufficient to assess the damage accurately. What is needed is a standardized damage assessment model to assist IS managers when investigating information system incidents.

Chapter 3 will discuss the method used to collect the necessary data to begin the process of establishing a model for damage assessment following information system intrusions.

Further, in Chapter 4 the data collected will be analyzed and assessed to determine the primary factors that are needed to build a DAM. Chapter 5 will discuss the results and model. It will also include limitations of the thesis and recommend some further research.

III. Methodology

Introduction

This research collected information necessary to propose a DAM for information system incidents. This chapter discusses the exploratory nature and method used to conduct the research. It further explains the development of the questionnaire and reasoning behind the questions. It also discusses the criteria used to select the subjects from whom the information would be gathered.

Research Method

The limited amount of research found relating to DAMs or methods directed this thesis towards an exploratory research project. No current model was found that could be addressed, expanded on, or validated. In addition, there was insufficient accurate and historical data to conduct a longitudinal study and propose an accurate model (Cooper and Schindler, 1998). For these reasons, an exploratory study was conducted to propose a model for future research and validation. To gather the necessary data a case study approach was utilized. The case study is the preferred research method for areas of study such as managerial, organizational, hypothesis development, and criminology (Yin, 1984; Dane, 1990). The development of a DAM relates to an IS manager's ability to perform an investigation in regards to a potential criminal act against an organization; hence, according to Yin (1984) a case study would be an appropriate method of research. Additionally, a case study, unlike a survey, typically has fewer numbers of subjects (Yin, 1984; Dane, 1990). Because the target subjects

for this study were upper-level managers, their scarcity significantly reduced the pool of available subjects. This case study used an experience questionnaire to probe the knowledge of the target subjects looking for areas of concern or ideas about performing IS damage assessments. The experience questionnaire is a very useful tool when attempting to generate new hypotheses, models, or ideas that require in-depth knowledge in areas that lack good secondary data, such as organizational records (Cooper and Schindler, 1998).

During the literature review, no reliable historical data could be found relating to DAMs and costs of information system incidents. One possible reason for the lack of reliable information, relating to information system incidents, is that organizations are averse to releasing this information, since it admits to having failed at information security and can be potentially damaging to the organization (Geis, 1991, Amoroso, 1999). Another reason, as described in Chapter 2, for the lack of historical data is the limited use of formal procedures or models by organizations to calculate the costs of information system intrusions (FBI, 1999). In order to collect the data required to build the DAM it was necessary to collect the information from subject matter experts using an experience questionnaire (Cooper and Schindler, 1998).

Questionnaire Development

Open-ended questions used in experience questionnaires are a good method for collecting data relating to ideas, *what* questions, and experiences (Cooper and Schindler, 1998). In addition, Yin (1984) discusses the importance of using questionnaires as a source of information when doing a case study. Kvale (1996) uses the analogy of a researcher as a miner, who must mine or dig for information using skillful techniques and questions. For this

research the information required to build a damage assessment model was contained in the tacit knowledge held by high-level information system and information security managers and required some mining to extract

The difficulty lies in extracting this tacit knowledge from managers and stating it explicitly. A formal structured questionnaire, using Likert scales and yes/no questions, is useful for gathering explicit knowledge, but lacks viability to gather tacit knowledge that is difficult for individuals to explain or that may not have a scalable answer (Kvale, 1996). Therefore, it was necessary to construct the questionnaire using open-ended questions which allow the subject to elaborate on questions (Kvale, 1996). To collect the data, a structured question and answer session was created to ensure the same questions were asked of all the subjects. The structured question and answer session allowed for a controlled session, yet the open-ended questions allowed the subjects to explain answers and gave the interviewer the ability to expand on a question if necessary (Yin, 1984; Cooper and Schindler, 1998).

To gather a broad range of experiences from a diverse group of upper-level managers a telephone question and answer session was chosen as the preferred method of data collection versus face-to-face. Had a face-to-face session been used, the pool of potential experts would have been limited to the driving distance the researcher could travel and therefore the telephone question and answer session was used to expand the potential pool of subjects to anyone that met the criteria and was willing to participate. A telephone question and answer session has some advantages and disadvantages. The advantages are the speed in which the data can be collected, the lower refusal rate, and fewer interruptions (Cooper and Schindler, 1998). The

disadvantages include the inability to use visual aids, attention span of subject if it is a long session, and possibility of a less thorough response (Cooper and Schindler, 1998). To alleviate as many of the disadvantages as possible no visual aids were used and the duration of the session was kept to less than 45 minutes. Additionally, to encourage a thorough response, the questionnaire was e-mailed to the subjects for their review before the actual telephone session.

Validity. During the literature review, no established validated constructs or instruments measuring the amount of damage could be found. Therefore, it was necessary to build the questionnaire and incorporate as much validity by using the information from the available literature. The available literature and research covered the constructs tangible, intangible, and IS manager's role, all in relationship to damage assessment. Rezmierski (1998) developed the two constructs of tangible and intangible as a way to categorize the damage caused by various information system incidents. The IS managers role as a construct came from various research showing that IS managers should be responsible for their information systems and understand the relationship between the systems and the business processes (Anderson, 1998; GAO/AIMD-96-84; Himebrook; 1997). Questions used to cover these constructs were open-ended and required the subject to expound on the topic. A group of four peers, all masters' students in Information Resource Management at the Air Force Institute of Technology with experience in the communication and information career field reviewed and commented on the questionnaire. This group evaluated the questionnaire to ensure the necessary questions were asked and that the questions covered the constructs identified during the literature review.

The final questionnaire was revised to incorporate the information gathered from the peer review.

Reliability. Reliability was more difficult to establish since the questions are open-ended and the research is exploratory (Cooper and Schindler, 1998). The open-ended nature of the questions and the need for explanation by the subjects meant that the responses would be varied. Additionally, the lack of scaled items was a result of the need to extract the tacit knowledge of each subject.

Questionnaire. The final questionnaire, see Appendix A, consisted of 26 questions, 15 of which where open-ended questions allowing the subject to explain and detail information related to damage assessments and information system incidents. The remaining questions consisted of yes/no questions and questions that gathered personal data and organizational data to determine the responsibility and scope of management and to ensure they met the criteria for being a subject. The questionnaire was reviewed by a group of peers before being finalized.

The open-ended questions were designed to answer the constructs of tangible, intangible, and manager's role. They included questions such as *Do you feel that it is necessary for an IS manager to be able to cost an IS intrusion? Please explain your answer* and *Given that an intrusion has occurred, please tell me what you feel are the areas that must be considered to determine the cost of the intrusion?* During the telephone session the subjects were encouraged to expand on any question regardless of whether it was open-ended or not.

Subjects

In order to conduct a successful question and answer session it is important to have subjects who possess the necessary information, subjects that understands their role in the organization, and subjects motivated to co-operate (Cooper and Schindler: 1998). For the purpose of this study, subjects that have been involved with information security and information systems over ten yours were chosen to increase the likelihood of them having a broad range of experience. In addition to ten or more years of experience, subjects in an upper-level management position were selected to provide a better understanding of the entire organization and the business processes. A desired trait was experience with some type of intrusion or information incident. This further expanded the knowledge base and would add to a more complete DAM. The idea was to find subjects who met these criteria and could use their knowledge and experience to look beyond tangible damage and begin to explore how an information system incident would affect intangible parts of a business and its business processes. Even with the individual criteria, it is necessary to expand the scope of the subject pool. Therefore, subjects were selected from various industries, four genres were selected: 1) military, 2) education, 3) private corporations, and 4) government organizational. These four provide a very diverse cross section of the business world. An example of the increased diverseness is that private organizations and some educational institutes are for profit organizations, while government and military organizations are not for profit organizations. This diverseness broadens the knowledge base of the subjects and helps provide for a more complete model.

Approach

Potential subjects were contacted via telephone and asked to participate in the question and answer session. Initially 15 subjects were contacted and asked to participate in the study, only one did not desire to participate. Those subjects that were willing to participate in the sessions were e-mailed a copy of the questionnaire before a telephone question and answer session to allow the subject ample time to review the questions and contemplate their answers. After the subject had time to review the questionnaire, an appointment was scheduled with each subject that allowed for 45 minutes of uninterrupted time to complete the telephone session. This presented the most difficult part of gathering the data. The IS mangers contacted were at in an upper-level management position and their time was very limited. One subject rescheduled the telephone session ten times due to the inability to work it into the hectic schedule of an IS manager. Two subjects, after originally agreeing to participate, were required to back out because of the lack of available time and high workload.

When the telephone session was conducted each subject was told they had the option to answer any or none of the questions and that they could terminate the session at their discretion. Additionally, it was explained to the subjects that their personal data, Section 1 of the questionnaire (see Appendix A), collected would not be included in the actual thesis. This information was used to help categorize and analyze the data. Before completion of the telephone session, subjects were asked if they could be contacted in the future for any additional questions or necessary follow-up sessions.

Summary

In order to build a damage assessment model that was as complete as possible subject matter experts were selected and an experience questionnaire was used. The subjects were individuals with over ten years of experience in the information system career field and were in an upper-level management position. Further, these individuals were selected from a broad range of organizational types adding additional knowledge and experience to the model. A questionnaire was created that provided the opportunity for the subjects to expand on questions providing answers that were as complete and comprehensive as possible. By using a telephone question and answer session, the pool of subjects was made even more diverse by opening the pool to all potential subjects across a much greater area.

Chapter 4 discusses the completed model and how the primary factors were derived. After, this Chapter 5 will provide a discussion of the results and provide some further areas of research relating to DAMs.

IV. Data Analysis and Results

Overview

This chapter displays the results of the data collected in the form of a damage assessment model. It will discuss the processes used to determine the primary factors that constitute the model and then further explain each factor giving definitions and examples. Additionally, this chapter will review other issues pertinent to IS damage assessments addressed by subjects.

Primary Factors of the Model

The primary factors were developed with the information gathered from the subjects using an experience questionnaire. The answers provided by each subject were evaluated and condensed into key words or phrases. This often depended on the genre of the subject. An example is those individuals with a military background would use the word *mission* that would relate to the word *processes* or *business* in other genres. The key words and phrases provided by each subject were compared for likeness in meaning and content by the researcher and then combined to create a new list of refined factors. This list was again scrutinized and further refined by the research to develop the final list of primary factors. The final list was reviewed and compared to the information provided in original questionnaires by a group of three peers, all professional communication and information officers in the United States Air Force, to ensure none of the original ideas and factors were omitted. In order for a change to be made two out of three reviews had to agree on the proposed change. An attempt was made to ensure each

primary factor was mutually exclusive; however, due to the nature and variations of businesses some factors have influences that are not mutually exclusive. The following is the final condensed list of eight primary factors that make up the proposed DAM:

- recovery
- education/training
- business expenses
- productivity
- data
- lost revenue
- reputation
- human life

Recovery. 12 out of 12 subjects discussed some type of recovery process as a necessary item to assess. Recovery is the process that system administrators must take to restore an information system to the most current state prior to the incident. This includes the investigation to determine what was actually affected by the incident and the restoration of the system. If a system has accurate and current backups, then the process should be easier. This allows the system administrator to restore to the backup state and then manually input the data lost between time of backup to the current state. Recovery may also include issues such as reinstalling damaged software or replacing hardware that was damaged or confiscated by law enforcement for investigation. New hardware or software may be purchased to enhance security. User accounts may require rebuilding or new passwords created. The bottom line is that recovery includes all issues that must be accomplished to restore the information system to the most current state just prior to the incident. See Table 1, Damage Assessment Model Factors, for detailed explanation of sub-factors influencing the recovery process.

Education/Training. Education and training was only mentioned by 3 of the 12 subjects; however, its importance is a necessary factor when considering the various business processes and information systems an employee must know. As an investigation proceeds the need for

additional education and training within the organization may become evident. System administrators and information security personnel may not have the necessary skills to perform a thorough investigation. Therefore, it may be necessary to train them on more advanced investigation processes. In addition, future incidents may be avoided by properly training users. New security procedures may be necessary and implemented to secure the system. There will be a need to train and educate the users and system administrators on the new security processes. See Table 1, Damage Assessment Model Factors, for detailed explanation of sub-factors influencing the training and education factor.

Business Expenses. The business expenses are direct fees or costs that result from outages, which affect customers and other businesses. Again, only three of the subjects discussed this item as a factor to consider. These three subjects were all part of a commercial for profit organization. To them, the business expenses were very important assessment factors. An information system incident should impact the business processes of an organization. The impact may be in the area of direct fees or costs relating to a downed system. Each organization is impacted differently depending on their mission and business processes. These expenses may affect customer service centers due to increased customer concern from an outage. Each business process must be weighed against the incident and the impact. This includes business to business impact. Often a system outage could affect the inventory process of another company. See Table 1, Data Assessment Model Factors, for detailed explanation of sub-factors influencing the business expenses.

Productivity. All of the subjects discussed a form of productivity impact in one fashion or another. Organizations have costs relating to production. This may be service oriented, such as management or administration, or labor, such as assembly lines. When a system is impacted, the productivity of an organization will be impacted. It is necessary to determine ones business processes and evaluate how the organization's productivity will be impacted. See Table 1, Data Assessment Model Factors, for detailed explanation of sub-factors influencing the productivity factor.

Data. Again all 12 subjects discussed a form of data loss as a relevant factor. Data lost as a result of an information incident must be evaluated for the cost of recovery. Some data may not be recoverable nor cost efficient to recover. Some data may be stored on periodic backups that can be easily restored and other data must be re-entered manually. Either method produces a unique impact on an organization, in both time and man-power. In this information saturated society, some organizations make a living out of selling data. If this type of proprietary data is stolen the cost may be lost sales or lost customers. Again, businesses must evaluate their processes and how the data they store are impacted as a result of an information system incident. See Table 1, Damage Assessment Model Factors, for detailed explanation of sub-factors influencing the data factor.

Lost Revenue. As with business expenses only three subjects mentioned a form of lost revenue. Two other subjects mentioned factors that are loosely related. Business processes determine how a company makes money or accomplishes its mission. If a system is damaged it will be necessary to evaluate how this will impact the revenue generating processes of the

organization. See Table 1, Damage Assessment Model Factors, for detailed explanation of sub-factors influencing the lost revenue factor.

Reputation. Reputation was an important factor to only five of the twelve subjects. The military organizations were not overly concerned with reputation from the public's view point; however, they did concern themselves with how they were viewed internally by other military organizations. Two commercial organizations were more concerned with this than any other aspect of an incident. They were focused on ensuring that their reputation remained untarnished. The reputation is one of the most intangible factors of all. Some organizations found that their reputation was the most important part of their business, while others did not even consider it. Quantifying a reputation requires the ability to know how customers and future customers influence the business. According to one subject questioned, a member of a financial institution, it is necessary to understand the relationship between customer and business and the impact system outages may have on the customer. This may be extremely difficult to do. In addition, the reputation of an organization may influence the quality of employees available or willing to be hired by that organization. Subjects suggested that if an organization has a reputation as being insecure and vulnerable that it may not attract customers or high quality employees. See Table 1, Damage Assessment Model Factors, for detailed explanation of sub-factors influencing the reputation factor.

Human Life. Lastly, human life may be impacted by information system incidents. Only one subject considered this as a factor; however, upon examination it was determined that impact on human life was an important factor that should be considered. Though this factor is

important, it is also understood that few organizations will need to concern themselves with this factor. The military was the primary organization concerned with it. If systems go down military missions may be aborted that cost the lives of both military and civilians. In addition, if mass transportation systems are impacted by an incident the result may be accidents resulting in both deaths and injuries. There is also a potential impact on the morale and family life of information security personnel who work long hours and are often on call 24 hours a day. A high rate of incidents and low availability of workers puts an undue strain on those currently employed. See Table 1, Damage Assessment Model Factors, for detailed explanation of sub-factors influencing the human life factor.

Additional Factors. As the list of factors was narrowed down, it was evident that certain issues were prevalent throughout. One issue that touched upon almost every aspect of the tangible issues was man-hours. Regardless if the issue was investigation, hardware, or recovery man-hours were a consideration. Therefore, man-hours as a model factor were eliminated. Likewise, key business processes were a factor of the model that was soon removed, since it was determined to be an underlying issue of the entire model. In order to assess the damage it would be necessary for any organization to have a full understanding of their key business processes and how the processes are related to the organization's information systems. The need to understand the business processes became obvious as the model began to take shape and more information was reviewed.

A very interesting and important issue mentioned by ten out of eleven people (only eleven people answered this question) was that the investigation process was not an IS

manager's responsibility. Rather, it fell at a lower level, such as system administrators or information security personnel. However, nine of these ten subjects said that it was an IS manager's responsibility to know how to cost or assess the damage of an IS incident. The overwhelming feeling and rationale was that costing or damage assessment is a business issue and that it goes beyond the technical investigation and requires an upper-level manager that understands the business processes and how they relate to information systems.

Proposed Damage Assessment Model

Figure 3 depicts a graphical representation of the proposed information system incident DAM based on the data collected. The business processes of an organization form the foundation for the DAM. On top of the business processes are the information systems that support the business processes. As an incident occurs, the relationship between the business processes and the primary factors must be established. Once this is done, the IS manager must determine how each factor is influenced by the information systems. Since the foundation of the DAM is the business processes, each organization will have unique damage assessment

procedures built using the business processes, information systems impact, and DAM.

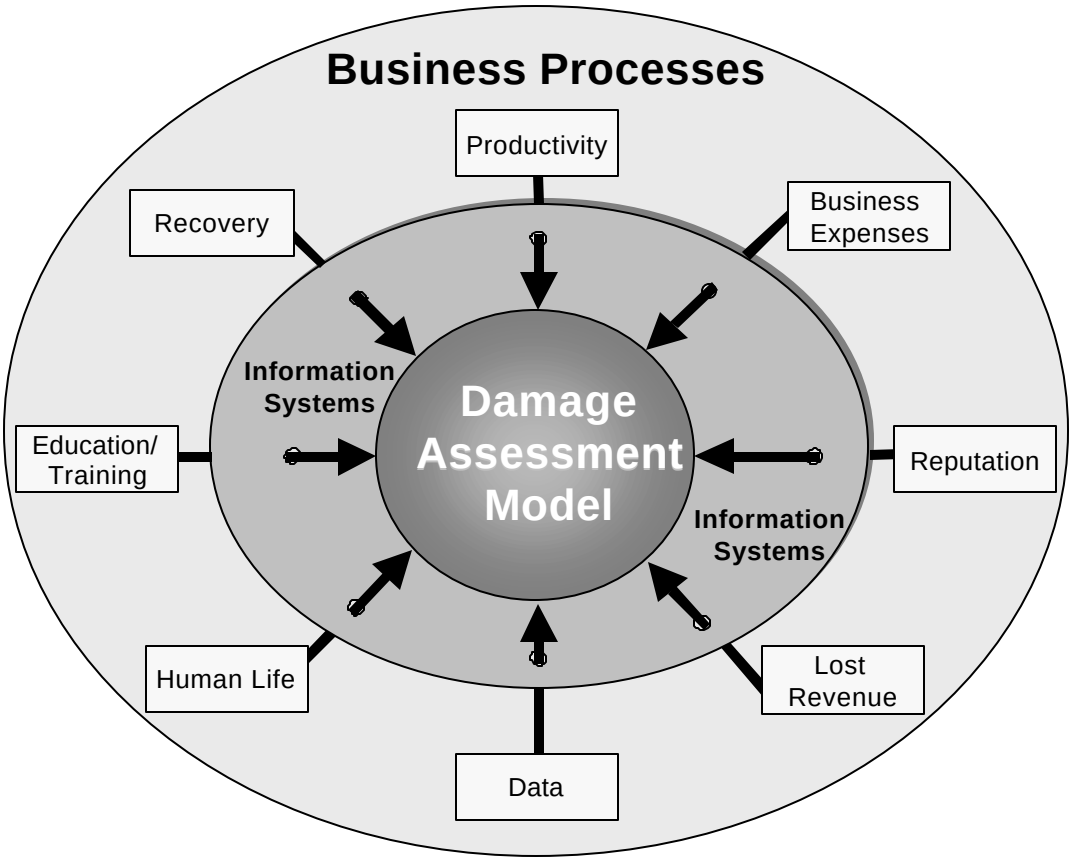

Figure 3 : Damage Assessment Model

The primary factors are further broken down into multiple sub-factors. Table 1 below provides a close look at each primary factor and its specific sub-factors. The sub-factors further define the primary factors allowing a more detailed assessment. They also provide an easier way to match business processes with a primary factor within the DAM.

Table 1: Damage Assessment Model Factors

Recovery	Investigation	Investigation involves all aspects of the process necessary to determine what actually happened and assess what needs to be fixed. This includes such things as intrusion detection, determining the damage, incident handling. Investigation will often continue well beyond the time of the actual incident.
	Restore	Network servers, desktop computers, routers, bridges, gateways and any other device altered as a result of the IS incident must be restored to its original state just prior to the incident. This could be done using a good backup, rebuilding a system, or purchasing new. In addition if a system is restored by backup there is usually a difference between the backup and current state when the system was altered. It is necessary to restore the system to current state.
	Software/ Hardware	In the event that an information system incident my damage software or even hardware it must be replace. This could happen due to altered disk drives causing unrecoverable damage to software. This could also be hardware confiscated, by law enforcement, for litigation that must be replaced. It can also include new hardware or software necessary to improve security of the IS.
	Consultants/ Contractors	During the investigation it may be necessary to hire outside help to perform a thorough investigation or repair of your system in areas which your organization does not have the expertise. Example: If a hard drive is damaged during the incident, it may require a clean-room facility to recover data.
	Accounts	If password files have been compromised, new passwords must be generated and all users must retrieve and reenter the new passwords. Also, involved in this is the need to regenerate accounts if backups do not have the necessary information. Users data stored on file servers may be corrupt and therefore restored or recreated.

Table 1(cont.): Damage Assessment Model Factors

Education/ Training	System Administrator/ Information Security Personnel	If an incident occurs it may be necessary to send or provide updated training to system administrators or information security personnel to ensure proper recovery or prevent future incidents. They may also require education or training in investigating incidents to ensure they are investigated properly and thoroughly.
	Employee COMSEC/INFOSEC	Following an incident, it is often necessary to educate employees on proper information security and computer security issues. They may need education on password generation and protection, data security, and system security. This could be basic how-to training on current systems or for new systems installed because of the incident.
Business Expenses	Customer Service	When a business or organization encounters an IS incident there will be business practices that are affected. Depending on the defined business practices affected will determine the impact on customers. Examples: Financial institutions may have to pay late fees, overdraft fees, and other fees associated with accounts affected by a system outage. Military organizations may not be able to perform a critical mission, launch aircraft, deploy troops, and other related mission needs. Over all, customer support facilities may be inundated with calls causing major problems.
	Business to Business	Business to business applications may be impacted by a system problem. All aspects of an organization that affect or are affected by an outside business must be investigated to ensure proper operations. Organizations are increasingly going to just-in-time inventories. If an inventory system shuts down then JIT may fail causing loss of sales or worse customers. Government relies on communication to do its job effectively. If a mode of communication should go down they could be adversely affected by this

Table 1(cont.): Damage Assessment Model Factors

Productivity	Mission Impact	Organizations that use IS or IT in their production could be affected. An organization must define its key processes to determine the extent of impact. Examples: Military may not be able to launch aircraft, deploy troops, perform certain actions or drop bombs without proper IS. A business may not be able to keep an assembly line running if certain information systems are impacted.
	Downtime	User downtime can occur if an IS is impacted. Many organizations are reliant on IS to do daily functions. If these systems go down, personnel are often left with little or nothing to do. Other times we resort to performing the functions on paper or other methods that must be later entered into the system.
	Communication	Currently our communication systems are dependent on technology. Information technologies control telephone systems, e-mail systems, and postal systems. Each system requires large amounts of IS to support its continued processing. In the event an IS happens in an organization there can be an impact on the communication process. This should be evaluated and assessed.
Data	Restoring	Lost data must be restored and is often restored from backup tapes. This may include cost of sending hard drives or storage devices to outside facilities that must restore the device.
	Re-Entering	Data that could not be restored or had been accumulated between the last back up and the current state of the system at the time of the incident must be re-entered. This impacts the functions of an organization since they must do this while at the same time continuing their current processes operational.
	Unrecoverable Data	It may not be possible to recover certain data. This includes data that no longer exists in paper or hardcopy format and the only copy was on the system affected by the incident. The cost of such data and its impact on an organization would need to be calculated.

	Proprietary Data	Data owned by an organization that is used for resale may be tampered with or stolen. If stolen these data loss value. Proprietary data is crucial to the operation of some organizations.

Table 1(cont.): Damage Assessment Model Factors

Lost Revenue	Lost Sales	IS incidents affect many parts of an organization. Determining the potential impact on sales is crucial to obtaining a true damage assessment. This requires an organization to understand its roles and key processes.
	Lost Customers	Like lost sales, a customer could be lost due to systems failing to work properly. Financial organizations that use the Internet to perform tasks could lose customer base if they can not keep their Internet services running or secure.
Reputation	Consumer/Public Confidence	The reputation of organizations is very susceptible to damage. In many cases a name and the quality behind the name is the most important part of an organization. If people loss confidence in the organization or its ability to perform then it may be impacted. This is true for both government and commercial organizations.
	Quality Employees	If the reputation of an organization is severely tarnished due to a publicized or known IS incident, the view may be that the organization is not an acceptable place of employment. This may result in a reduced pool of qualified employees. This is something that though necessary to consider is very difficult to evaluate and assess.
Human Life	Loss of Life	Though a very unlikely occurrence in many areas this is an issue in military area and even in some other government areas. Military missions could be impacted because of an incident that would result in the loss of life. A support or search and rescue mission may be aborted because of lack of information system support resulting in the loss of life. Mass transportation systems could be affected and cause potential loss of life due to accidents or catastrophes.

	High work load of ERT members	This is a direct result of the high rate of IS intrusions and incidents. Many of these teams are undermanned and overworked causing undue stress and hardship on families. Some experienced and highly qualified team members are on call 24/7/365.

Summary

The damage assessment model consists of eight primary factors all reliant upon the understanding of the business processes of the organizations. It is an IS manager's responsibility to learn the business processes and be able to use them when performing a damage assessment. The model further breaks down the primary factors into more detailed sub-factors that refine and help define the primary factors. Chapter 5 will discuss the issues relating to the results. It will also provide some recommendations based on this research and model.

V. Discussion

Overview of Model

The use of information technology is rising rapidly and along with it, the number of reported IS incidents. To combat the rising rate of incidents and to protect their assets businesses are spending billions of dollars annually on information security products, in many cases without the ability to justify the need or cost. According to the FBI/CSI 1999 survey, of the organizations surveyed that showed a loss from IS incidents, only 31 percent had the ability to calculate the loss. Yet, they spend billions of dollars without even knowing what damage has occurred when confronted with an IS incident. Information system managers are responsible for the information systems and understanding the how these systems relate to business processes of the organization. Without properly assessing the damages caused by information system incidents there is a significant potential for loss or waste to an organization's budget and reputation. All twelve subjects questioned said they would benefit considerably from a formal method and DAM, yet only one had a formal method for assessing damages and none of the others were in the process of developing one.

The upper-level managers provided a vast amount and broad spectrum of information into what a business considered important when involved assessing the damage of an information incident. Their views expressed the business, technological, and security concerns that an organization must deal with on a daily basis. The information they provided was

condensed into eight primary factors that are further broken down to secondary and more detailed factors providing a starting point for building a formal and standardized DAM.

Two factors influencing damage assessment were brought up repeatedly during the question and answer sessions; these factors were man-hours and business processes. These two factors were a common thread throughout many of the other factors and therefore were not included as primary factors but are rather explained as key issues that must be considered to successfully accomplish a damage assessment. The first, man-hours, was a major factor in almost every primary and secondary factor. For example, it takes man-hours to accomplish the recovery of the system, it takes man-hours to investigate the incident, and it takes man-hours to assess the data lost.

The second overarching factor and the most important issue was the need for organizations to define their business processes. Without well-defined business processes it is highly unlikely an organization could conduct a successful and complete damage assessment. Business processes underlie every primary factor and are required for managers to assess the true impact on an organization. Without defining the business processes an organization would be unable to determine loss in productivity, lost revenue, or business expenses.

One interesting result of the questionnaire was that, almost unanimously, the subjects felt that the investigation of an incident was not the responsibility of the IS manager, but costing or assessing the damage of an incident was an IS manager's responsibility because of their understanding of the organizations business processes and issues. Simply allowing system administers or information security personnel to cost or assess the extent of damage to an

organization would often limit the damage to only the information technology and system recovery issues and not to the overall costs to an organization. The damage an organization faces is often much greater than the simple calculation of the man-hours needed to rebuild a server or to restore from a backup. Rezmierski (1998) emphasizes the fact that the intangible costs from an IS incident can far exceed the tangible. Many of the intangible costs are derived from the knowledge of organizational business processes.

Recommendations

Damage assessment is a complicated and very labor intensive, yet necessary task. Current industry methods of conducting damage assessments are ad hoc at best with only a few organizations even capable of assessing the cost resulting from an incident (FBI, 1999). A standard methods of conducting damage assessments would provide an excellent starting point to better understand the true cost of IS incidents and the impact they have on an organization. Information system managers responsible for costing damage assessments need to develop a formal process for conducting damage assessments. This process must be rigid enough to meet the organization's needs at the same time it must be flexible enough to encompass the variety of IS incident.

The first and most important thing an IS management must do is define the organization's key business processes. Once this is done the IS manager can then use the DAM to develop a formal process for conducting damage assessments. The model can then be expanded or contracted to meet the needs of each organization. Many of the factors involved with the DAM will affect every organization yet there are some that only fit a few. Loss of life is

one factor that would more than likely not affect a financial institution, yet a military organization should be conscious of this factor when conducting a damage assessment.

Implications

This information system incident DAM is a foundation for an area or research that requires further study and refinement. A great deal of research has been done in the areas of risk analysis, information security, and information management. However, this research has been focused on prevention and not on the damage assessment following an incident. Information systems are vulnerable and prevention is not enough for IS managers to focus on. Information managers must be prepared to answer what went wrong and what was the impact on the business after an incident has occurred. Researchers should continue the exploration and investigation into this area to refine, understand, and potentially standardize the damage assessment process.

This model also provides IS managers with an additional tool to assist in the daily endeavor to manage the information systems. By using the model and the checklist, they can create a damage assessment procedures that will benefit their organization. This model can help standardize the damage assessment process across industries to better understand the damage caused by information incidents. By better understanding the damage caused organizations can budget accordingly, potentially saving millions of dollars in unnecessary spending. Additionally, the model provides managers with a new planning tool to recover from an information system incident.

Limitations

Although a model was developed successfully there are some limitations. First, the low number of subjects used was a limiting factor. Secondly, the available data relating to actual damage assessments were limited and in some cases not available leading to the development of a questionnaire with limited validity and reliability. Lastly, the questionnaire was administered via telephone and therefore introduced potential error in transcribing and ensuring everything was captured during the conversation with the subject.

Recommendations for Future Research

This thesis defined eight primary factors that constitute the proposed damage assessment model for information intrusions. Further research in this area should take each primary factor and develop a valid and reliable instrument consisting of the sub-factors as items within the instrument. These factors and instruments should be validated against actual intrusions to further enhance the functionality of the DAM. As the DAM is refined, validated, and checked for reliability a cost model should be developed.

One important issue for further research was suggested by one of the subjects. The subject suggested that an industry standardization body such as IEEE or Gartner Group should validate a DAM to establish an industry standard for damage assessment. All the subjects, participating in this questionnaire, agreed that a standardized model would be a significant tool for IS managers to have in their possession.

Conclusion

The exploratory research conducted to develop the damage assessment model in this thesis is significant, in that it is one of the first attempts at standardizing the process of damage assessments across the IS/IT industry. It provides the foundation for future research to validate and enhance the model for a more accurate understanding of the true damage to businesses caused by IS incidents. This model will also contribute to IS manager's understanding of IS incident's impact on the business processes. Business processes are the foundation to the model providing insight into how information systems impact the functions of an organization. Because of an information system manager's understanding of the business processes and information infrastructure of the organization, they should be responsible for assessing the damage and costing an IS incident. The DAM developed is one more tool they have to accomplish this colossal task.

Appendix A

Structured Questionnaire

The purpose of this interview is to obtain opinions and information from senior information technology individuals related to the assessing the true costs of an information system intrusion. This information will be used to help create a standardized model or process for accomplishing an information damage assessment.

Section 1 information **will not** be disclosed in the final report and will only be used to categorize the information collected. Please take time to consider the questions carefully and answer them as fully as possible. If more time is needed, subsequent interviews may be accomplished.

1. Personal & Organization Information

1.1. Interviewee _____

1.2. Organization _____

1.3. Position in Organization _____

1.4. Time Employed with organization _____

1.5. Time in IT/IS career field _____

2. Organization's Information System Data

2.1. What are the primary types of information systems your organization uses, including Internet/Extranet/Networks?

_____

_____

_____

_____

_____

_____

_____

3. Organizational Intrusion History

For the purposes of this study, an intrusion is defined as "a calculated and intentional attempt by an individual or organization to access an information system they do not have permission or rights to access."

3.1. Have there ever been intrusions on your organizations IS?

YES (continue with 3.1.1) NO (go to 3.2)

3.1.1. If YES to 3.1, then,

3.1.1.1. Were you working in your current position when the intrusion occurred?
YES NO

3.1.1.2. Were you actively involved with the detection and handling of the intrusion? **YES NO**

3.1.1.3. Do you feel your organization was prepared to handle an intrusion?

YES NO

3.1.1.4. Since being attacked, is your organization better prepared to handle future intrusion attempts?

YES NO

3.2. If NO to 3.1, do you feel your organization is capable of handling an intrusion of your IS?

YES NO

3.3. Does your organization have intruder detection software or hardware installed?

YES NO

3.4. Does your organization have formal procedures for system administrators to follow to handle an intrusion?

YES NO

3.5. If an intrusion should occur, does your organization intend on involving law enforcement?

YES NO

3.6. Does your organization have a formal standardized method for calculating the cost of an IS intrusion?

YES NO

3.7. Do you believe an information system intrusion is inevitable?

YES NO

4. Professional Opinion

4.1. What are you're your biggest fears in regards to an IS intrusion: Inside job or outside hacker? Why?

4.2. Do you feel that it is necessary for an IS manager to be able to cost an IS intrusion? Please explain your answer.

_____

_____

4.3. Do you think that IS managers, as a whole, are sufficiently trained to investigate an IS intrusion?

YES NO

4.3.1. If NO, should they be and why or why not? _____

_____

_____

_____

_____

_____

_____

_____

_____

_____

4.4. Do you think that IS managers are sufficiently trained to cost an IS intrusion?

YES NO

4.4.1. If No, should they be trained and why or why not?

_____

_____

_____

_____

_____

_____

4.5. Do you actively consider the potential loss to your company, organization or institution from an IS intruder?

YES NO

4.6. Do you believe your organization would benefit from a standardized method to conduct damage assessment?

YES NO

Please explain your answer. _____

4.7. What are some of the impediments encountered when conducting a damage assessment?

5. Intrusion Cost Assessment

5.1. Given that an intrusion has occurred, please tell me what you feel are the areas that must be considered to determine the cost of the intrusion? (list all areas that come to mind, examples: man-hours for recovery, rebuilding system, generating new passwords, company reputation, customer confidence, etc.)

5.1.1. Tangible Costs (man hours to recover, systems failures, etc.):

5.1.2. Intangible Costs (organizational reputation, lost sales, etc.) _____

Appendix B

Table 2: Damage Assessment Model: Recovery

Recovery	Investigation	Investigation involves all aspects of the process necessary to determine what actually happened and assess what needs to be fixed. This includes such things as intrusion detection, determining the damage, incident handling. Investigation will often continue well beyond the time of the actual incident.
	Restore	Network servers, desktop computers, routers, bridges, gateways and any other device altered as a result of the IS incident must be restored to its original state just prior to the incident. This could be done using a good backup, rebuilding a system, or purchasing new. In addition if a system is restored by backup there is usually a difference between the backup and current state when the system was altered. It is necessary to restore the system to current state.
	Software/ Hardware	In the event that an information system incident my damage software or even hardware it must be replace. This could happen due to altered disk drives causing unrecoverable damage to software. This could also be hardware confiscated, by law enforcement, for litigation that must be replaced. It can also include new hardware or software necessary to improve security of the IS.
	Consultants/ Contractors	During the investigation it may be necessary to hire outside help to perform a thorough investigation or repair of your system in areas which your organization does not have the expertise. Example: If a hard drive is damaged during the incident, it may require a clean-room facility to recover data.

	Accounts	If password files have been compromised, new passwords must be generated and all users must retrieve and reenter the new passwords. Also, involved in this is the need to regenerate accounts if backups do not have the necessary information. Users data stored on file servers may be corrupt and therefore restored or recreated.

Table 3: Damage Assessment Model: Education/Training and Business Expenses

Education/ Training	System Administrator/ Information Security Personnel	If an incident occurs it may be necessary to send or provide updated training to system administrators or information security personnel to ensure proper recovery or prevent future incidents. They may also require education or training in investigating incidents to ensure they are investigated properly and thoroughly.
	Employee COMSEC/INFOSEC	Following an incident, it is often necessary to educate employees on proper information security and computer security issues. They may need education on password generation and protection, data security, and system security. This could be basic how-to training on current systems or for new systems installed because of the incident.
Business Expenses	Customer Service	When a business or organization encounters an IS incident there will be business practices that are affected. Depending on the defined business practices affected will determine the impact on customers. Examples: Financial institutions may have to pay late fees, overdraft fees, and other fees associated with accounts affected by a system outage. Military organizations may not be able to perform a critical mission, launch aircraft, deploy troops, and other related mission needs. Over all customer support facilities may be inundated with calls causing major problems.
	Business to Business	Business to business applications may be impacted by a system problem. All aspects of an organization that affect or are affected by an outside business must be investigated to ensure proper operations. Organizations are increasingly going to just-in-time inventories. If an inventory system shuts down then JIT may fail causing loss of sales or worse customers. Government relies on communication to do its job effectively. If a mode of communication should go down they could be adversely affected by this

Table 4: Damage Assessment Model: Productivity and Data

Productivity	Mission Impact	Organizations that use IS or IT in their production could be affected. An organization must define its key processes to determine the extent of impact. Examples: Military may not be able to launch aircraft, deploy troops, perform certain actions or drop bombs without proper IS. A business may not be able to keep an assembly line running if certain information systems are impacted.
	Downtime	User downtime can occur if an IS is impacted. Many organizations are reliant on IS to do daily functions. If these systems go down, personnel are often left with little or nothing to do. Other times we resort to performing the functions on paper or other methods that must be later entered into the system.
	Communication	Currently our communication systems are dependent on technology. Information technologies control telephone systems, e-mail systems, and postal systems. Each system requires large amounts of IS to support its continued processing. In the event an IS happens in an organization there can be an impact on the communication process. This should be evaluated and assessed.
Data	Restoring	Lost data must be restored and is often restored from backup tapes. This may include cost of sending hard drives or storage devices to outside facilities that must restore the device.
	Re-Entering	Data that could not be restored or had been accumulated between the last back up and the current state of the system at the time of the incident must be re-entered. This impacts the functions of an organization since they must do this while at the same time continuing their current processes operational.
	Unrecoverable Data	It may not be possible to recover certain data. This includes data that no longer exists in paper or hardcopy format and the only copy was on the system affected by the incident. The cost of such data and its impact on an organization would need to be calculated.

	Proprietary Data	Data owned by an organization that is used for resale may be tampered with or stolen. If stolen these data loss value. Proprietary data is crucial to the operation of some organizations.

Table 5: Damage Assessment Model: Lost Revenue, Reputation, and Human Life

Lost Revenue	Lost Sales	IS incidents affect many parts of an organization. Determining the potential impact on sales is crucial to obtaining a true damage assessment. This requires an organization to understand its roles and key processes.
	Lost Customers	Like lost sales, a customer could be lost due to systems failing to work properly. Financial organizations that use the Internet to perform tasks could lose customer base if they can not keep their Internet services running or secure.
Reputation	Consumer/Public Confidence	The reputation of organizations is very susceptible to damage. In many cases a name and the quality behind the name is the most important part of an organization. If people loss confidence in the organization or its ability to perform then it may be impacted. This is true for both government and commercial organizations.
	Quality Employees	If the reputation of an organization is severely tarnished due to a publicized or known IS incident, the view may be that the organization is not an acceptable place of employment. This may result in a reduced pool of qualified employees. This is something that though necessary to consider is very difficult to evaluate and assess.
Human Life	Loss of Life	Though a very unlikely occurrence in many areas this is an issue in military area and even in some other government areas. Military missions could be impacted because of an incident that would result in the loss of life. A support or search and rescue mission may be aborted because of lack of information system support resulting in the loss of life. Mass transportation systems could be affected and cause potential loss of life due to accidents or catastrophes.

	High work load of ERT members	This is a direct result of the high rate of IS intrusions and incidents. Many of these teams are undermanned and overworked causing undue stress and hardship on families. Some experienced and highly qualified team members are on call 24/7/365.

Appendix C

Table 6:Damage Assessment Checklist

Primary Factor	Sub-factors	Business Processes*
Recovery	Investigation	
	Restore	
	Software/ Hardware	
	Consultants/ Contractors	
	Accounts	
Education/ Training	System Administrator/ Information Security Personnel	
	Employee COMSEC/INFOSEC	
Business Expenses	Customer Service	
	Business to Business	
Productivity	Mission Impact	
	Downtime	
	Communication	
Data	Restoring	
	Re-Entering	
	Unrecoverable Data	
	Proprietary Data	
Lost Revenue	Lost Sales	
	Lost Customers	
Reputation	Consumer/Public Confidence	
	Quality Employees	
Human Life	Loss of Life	
	High work load of ERT members	

*** Business Processes:** Determined by organization. Must establish impact and relationship between processes and factors.

Bibliography

"About the Center." Center for Education and Research in Information Assurance and Security. Web site, http://www.cerias.purdue.edu/about.php3 (2 Nov 99).

Air Force Computer Emergency Response Team (AFCERT). "Mission and POC." Web page, http://afcert.csap.af.mil/mission.html (8 Jun 99).

Amoroso, Edward. Intrusion Detection: An Introduction to Internet Surveillance, Correlation, Traps, Trace Back and Response. Sparta, NJ: Intrusion.net Books, 1999.

Anderson, Kent. "Intelligence-based Threat Assessment for Information Networks and Infrastructures." Global Technology Research, Inc. White paper, n. pag. 11 Mar 98.

Bureau of Labor and Statistics. 1998-1999 Occupational Outlook Handbook. Online Handbook, http://www.bls.gov/oco/ocos042.htm. (14 Nov 99).

CERT®/CC "Incident Report." Statistics on WWWeb page, n. pag. http://www.cert.org/stats/cert_stats.html (15 Nov 99).

-----. "Steps for Recovering from a UNIX Root Compromise." Web page, n. pag. http://www.cert.org/tech_tips/root_compromise.html (27 Apr 99).

Colkin, Eileen. "Grainger Sees E-Commerce Payoff." InformationWeek Online. http://www.informationweek.com/shared/printableArticle?doc_id=IWK19990429S0003. (30 Apr 99).

Cooper, Donald R. and Schindler, Pamela S. Business Research Methods. Boston: Irwin/McGraw-Hill, 1998.

Dalton, Gregory. "E-Business Evolution." InformationWeek, 737: 50 (7 Jun 99).

Dane, Francis C. Research Methods. Pacific Grove, CA: Brooks/Cole Publishing Company, 1990.

Denning, Dorthy E. Information Warfare and Security. Reading, MA: Addison-Wesly, 1999.

Department of the Air Force. Computer Securities Training Instruction. AFI 33-204. Washington: HQ USAF, Mar 98.

DiDio, Laura. "Computer Crime Costs on the Rise," Computer World: 23-25 (20 Apr 98).

Dyson, Esther. "A Map of he Network Society." New Perspective Quarterly, 14: 25-28 (Spring 97).

Geis, Gilbert. "The Case Study Method in Sociological Criminology." A Case for the Case Study. Ed. Joe R. Feagin, Anthony M. Orum, and Gideon Sjoberg. Chapel Hill, NC: The University of North Carolina Press, 1991.

Government Accounting Office/Accounting and Information Management Division. Information Security: Computer Attacks at Department of Defense Pose Increasing Risks. Report Series GAO/AIMD-96-84. Washington: GPO, 1996.

Government Accounting Office/Accounting and Information Management Division. Information Security: Computer Hacker Information Available on the Internet. Report Series GAO/T-AIMD-96-108. Washington: GPO, 1996.

Hafner, Katie and Markoff, John. Cyber Punks: Outlaws and Hackers on the Computer Frontier. NY: Touchstone, 1992.

Hamilton, Caroline R. "Risk Management and Security," Information Systems Security, vol. 8, issue 2: 69-78 (Summer99).

Harvey, Christopher. "CERT—Computer Emergency Response Team," Computer Networks and ISDN Systems, 23: 167-170 (November 1991)

Himebrook, Leslie F. A Model For Determining Information to be Captured Regarding Unauthorized Computer Entry of an Air Force Compute System. MS thesis, AFIT/GIS/LAS/97D-1. School of Systems and Logistics, Air Force Institute of Technology (AU), Wright-Patterson AFB OH, December 1997.

Howard, John D. An Analysis of Security Incidents on the Internet: 1989-1995. Ph.D. dissertation. Carnegie Mellon University, Pittsburgh PA, April 1997.

Internet Engineering Task Force. Site Security Handbook. RFC 2196. September 1997.

"IT Capital Outlay Growing." Electronic News, 42: 48 (16 Dec 96).

Kammer, Raymond G. Statement before the House Science Subcommittee on Technology, Text on Web page http://www.house.gov/science/kammer__062499.htm, n. pag. 24 Jun 99.

Kratz, Martin P.J. "Canada's Computer Crime Laws: Ten Years of Experience." Information Systems Security: Facing the Information Society of the 21st Century. Ed. Sokratis K. Katsikas and Dimitris Gritzalis. London: Chapman & Hall, 1996.

Kvale, Steinar. Interviews : An Introduction to Qualitative Research Interviewing. Thousand Oaks, CA: Sage Publications, 1996.

Martell, Duncan. "Survey Looks at Cost of Information Technology." Bloomberg News. Digital Newspaper, http://wwwcomputernewsdaily.com/267_092497_102206_10495.html. (18 Nov 99).

McCune, Jenny C. "How Safe is Your Data?" Management Review: 17-22 (October 1998).

Mosquera, Mary. "Computer Attacks Spreading." TechWeb. Digital Newspaper, http://www.techweb.com/wire/story/TWB19991118S0003. (18 Nov 99).

Ott, Jeffrey L. "Preparing for the New Millennium." Information Systems Security: vol. 8: 3-6, (Summer 1999).

Pascal, Blaise. "Great Books of the World: Pascal." Encyclopedia Britannica, 33. Ed. Robert Maynard Hutchins. Chicago: University of Chicago Press, 1986.

Pethia, Richard. "Testimony before the Permanent Subcommittee on Investigations." Web page at CERT®/CC. http://www.cert.org/docs/ (8 Jun 99).

Power, Richard. "1999 CSI/FBI Computer Crime Security Survey." Computer Security Issues & Trends, vol. V, no. 1. San Francisco, CA: Computer Security Institute, Winter 1999.

Rezmierski, Virginia and others. Final Report: Incident Cost Analysis and Modeling Project. Michigan: University of Michigan Press, 1998.

Ruben, Aviel D., Geer, Daniel and Ranum, Marcus J. Web Security Sourcebook. NY: John Wiley & Sons, Inc., 1997.

Rutrell, Yasin. "Think Twice Before Becoming a Hacker Attacker." InternetWeek, 745: 30 (Dec 98).

Schwartz, Feffrey. "IT Healthy in Finance Arena." InformationWeek, 771: 19 (28 Jul 99).

Shulman, Richard. "Technology—Make Plans for E-Business." Supermarket Business, 54: 33-34 (1 Aug 99).

Sterling, Bruce. The Hacker Crackdown: Law and Disorder on the Electronic Frontier. NY: Bantam Books, 1992.

Straub, Detmar W. "Coping With Systems Risk: Security Planning Models for Management Decision Making(n1)," MIS Quarterly, vol. 22, issue 4: 441-469 (Dec98).

"Technology." Journal of Accountancy, 187: 16-17, (Jan 99).

Toigo, Jon. Disaster Recovery Planning: For Computers and Communication Resources. NY: John Wiley & Sons, Inc., 1996.

Triendle, Robert. "Sony Restructures to Embrace Digital Economy." Research Technology Management, 42: 4-5 (Sep/Oct 99).

Trigaux, Robert. "Hackers: Hidden Dangers." Web page, n. pag. http://www.sptimes.com/Business/61698/Hackers_third_in_a_s.html. 10 Aug 99.

Vatis, Michael A. "Cybercrime, Transnational Crime, and Intellectual Property Theft." Statement before Congressional Joint Economic Committee, n. pag. 24 Mar 98.

Vatis, Michael A. "NIPC Cyber Threat Assessment" Statement before Senate Judiciary Committee: Subcommittee on Technology and Terrorism. 6 Oct 99.

Violino, Bob. "The Security facade," InformationWeek: 68-69 (21 Oct 96).

Willemse, Nicolene and du Toit, Adeline S.A. "Determining the Value of Information—A Pragmatic Approach." South African Journal of Library & Information Science, 64: 8-14 (March 1996).

Wright, Marie A. "The Need for Information Security Education." Computer Fraud & Security: 14-17 (Aug 98).

Vita

Captain Mark D. Horony was born 1 November 1965 in Bad Constance Military Hospital Stuttgart, Germany. He graduated from James Madison High School, San Antonio TX in 1984. He enlisted and entered active duty AF in 1985. He was selected for the Airmen Education and Commissioning Program and attended Texas A&M University graduating in 1991 with a Bachelor of Science Degree in Computer Science. After graduation from Texas A&M he attended officer training school and was commissioned into the AF on 3 June 1992.

His first assignment was to Tinker AFB as a programmer for AWACS operational software. During this assignment, he was deployed multiple times in support of Operation Southern Watch and Operation Northern Watch. His next assignment was to HQ Air Intelligence Agency as a systems integrator and network architect. He entered the School of Logistics and Acquisition Management, AFIT in May 1998. Upon graduation from the School of Engineering and Management, he will be assigned to the 375th Communications Squadron, Scott AFB.

Permanent Address: 6426 Falls Church
San Antonio, TX 78249

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	December 1999	Master's Thesis

4. TITLE AND SUBTITLE
Information System Incidents: The Development of a Damage Assessment Model

5. FUNDING NUMBERS

6. AUTHOR(S)
MARK D. HORONY, Capt, USAF

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Air Force Institute of Technology
2950 P Street
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER
AFIT/GIR/LAS/99D-5

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
~~OASD/IAT~~
~~Mr. James Christy~~
~~1400 Defense Pentagon, Rm 1E757~~
~~Washington D.C. 20301-1400~~
~~(703) 602-9982~~
Jim Christy
ASDC3I/DIAP
1215 Jefferson Davis Highway, Ste 1104
Arlington VA 22202

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES
Advisor: David P. Biros, Major, USAF
AFIT/ENV (937) 255-3636 x4826
daivd.biros@afit.af.mil

12a. DISTRIBUTION AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

Information system (IS) incidents are on the rise. With low manning and under-trained information security specialists it is difficult for organizations to stop IS incidents from occurring. Once an incident has occurred it is the IS manager's responsibility to ensure that a full and accurate damage assessment has been accomplished. However, most IS managers lack the necessary tools to assess the damage from an incident.

This exploratory thesis developed an IS incident damage assessment model (DAM) that can be part of the IS manager's tool kit. During the development of the model, it became apparent that the model was supported by a foundation of business processes. Therefore, the most important thing an IS manager can do is define their organization's business processes and how they relate to information systems. The model is based on eight primary factors to considered: recovery, education/training, business expenses, productivity, data, lost revenue, reputation, human life.

Each factor is then further expanded into sub-factors that better define and explain the primary factors. These sub-factors can be directly mapped to business processes previously defined by the information system manager. The final product is an IS incident DAM tailored to the needs of the IS manager's organization

14. SUBJECT TERMS	15. NUMBER OF PAGES
damage assessment, computer intrusions, disaster recovery, cost analysis	74
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL