AN INFORMATION SECURITY RISK ASSESSMENT MODEL FOR PUBLIC AND UNIVERSITY ADMINISTRATORS

By
Victoriano Casas III

An Applied Research Project
(Political Science 5397)
Submitted to the Department of Political Science
Texas State University
In Partial Fulfillment for the Requirements for the Degree of
Masters of Public Administration
Spring 2006

Faculty Approval:

_____
Dr. Hassan Tajalli

_____
Dr. George Weinberger

_____
Mr. Dan O'Leary

DEDICATION

This is dedicated to my wife, Shelley.
Thanks for putting up with my late night writing.
Thank you for proofreading all my work.
Most of all thank you for your patience.
Con amor y cariño
~Victoriano~

TABLE OF CONTENTS

CHAPTER I. INTRODUCTION

The purpose of this paper is three fold. First this paper will explore the literature on information security in order to identify ideal components of a security program. Second, a survey on these ideal components will gather information security professionals' opinion on the most important elements of each component. Finally the results of a survey will provide input on an ideal information security risk assessment program for educational institutions and/or state and local government agencies.

Assessing the risk of information security in the public sector involves many steps. Once a program is in place, assessing the risk of the given organization is one of the first steps to assure the security of the data and its systems. For public administrators in state and local government, as well as public universities there is little research on conducting an effective risk assessment from the management to the operations to the technical controls. This research explores the literature on the history and background of the internet and cyber security. The research gives an introduction to an information security program and the laws and regulations on information security. Policies fundamental to an organization/university are discussed and eventually the ideal components of a risk assessment will be described.

Information security is often thought of as a computer technician or network administrator protecting computers with anti-virus software and some sort of network firewall. However, there is much more to information security than just the technical staff and the software. New malicious code, worms, and distributed denial of services are taking place in cyberspace at an exponentially faster level than ever before. In November

of 2005, iDefense released information that hackers have "unleashed a record-setting 6,191 keyloggers[1] in 2005" (Roberts 2005). Senior level executives in business and government are realizing that there is more to information security than just a computer technician installing anti-virus software. Companies must deal with the internal threat, the disgruntled employee; they must address fundamental security policies, and have a disaster recovery plan in place to be prepared for the worst.

Within the last five years security awareness and the interest of information security has grown in both large companies and the public sector. Recent worms and computer viruses, like SQL Slammer and Mimail, have caused millions of dollars in loss of productivity and the average computer user is now being forced to deal with security. CNN reported, in January 2003, that the SQL Slammer worm "grounded flights and blocked ATMs" (Sieberg and Bash 2003). Chances are if a person uses a computer that is connected to the Internet, that person probably has a username and password; if so, information security is just as much their business as it is the business of the information security staff.

Public administrators must realize the importance of information security and its place in public agencies. Computer and internet technology is advancing quickly and it is critical that administrators understand how an information security office shall work to protect its assets. This research shall serve as a guide to those public administrators who are unaware of the criticality of information security. It shall also assist in the understanding of the ideal components of a risk assessment as well as the structure of an information security program. University officials as well as public administrators in

[1] A keylogger can be hardware based or software based. Malicious keyloggers are programs that literally save every key stoke on a victim's computer. The malicious person can then access the keylogger remotely to obtain the user's passwords and other useful information.

state and local agencies can use the ideal components to address the needs of information security in their respective agencies.

The next chapter explores the literature and discusses the background of the Internet and the explosive growth of the technology as well as how public administrators are utilizing information security portals online to prepare and protect their data. Chapter III discusses the components of an information security program. Chapter III discusses the appropriate staff needed for an information security program, as well as the critical security polices needed for the structure of a complete information security program. Within chapter III, data classification, one of the ideal components of an information security risk assessment, is discussed in detail. Chapter IV discusses the various laws and regulation regarding information security. Although chapter IV does not go into great detail of each law, it is important that public administrators and university officials are aware of the various laws and regulation in their respective jurisdiction. Chapter V discusses the remainder of the ideal components of an information security risk assessment. Chapter V is divided into the following three subcategories, management controls, operational controls, and technical controls. Chapter VI discusses the conceptual framework used for this applied research project. Immediately following is chapter VII which discusses the methodology of this applied research project. Chapter VIII gives the results of the research, and finally chapter IX concludes the entire research project and brings this paper to a close.

CHAPTER II. BACKGROUND OF THE INTERNET & CYBER SECURITY

The Internet started out as a form of open communication. It was meant to share information between universities and the departments/agencies of the Federal Government. The Advanced Research Projects Agency Network (ARPANET) of the U.S. Department of Defense, what is now known to be the Internet, was developed as a backup plan in case other ways of communication were unavailable and also as a result of the USSR's launch of Sputnik. ARPA stood for Advanced Research Projects Agency[2] (Garfinkel and Spafford and Schwartz 2003). "Today the descendant of the ARPANET is known as the Internet" (Garfinkel and Spafford and Schwartz 2003, 269).

A. How the Internet works

The way the Internet works and how computers speak to each other on the Internet is by a protocol or language known to computers as Transmission Control Protocol/Internet Protocol (TCP/IP) (Feit 1999). TCP/IP has been insecure from the start. TCP/IP was designed for open communication and was never intended to secure or conceal information. "The technology was meant to *enable* communication, whereas security is the opposite. Security tries to *prevent* something from happening, or prevent people from doing something" (Schneier 2004, 13).

As the Internet got more and more popular, businesses and governments started to utilize it for trade and commerce. They not only utilized the Internet for communications, but also to transfer confidential and sensitive information from one machine to another. Today the Internet is used to transfer millions of dollars worldwide.

[2] Some referred to it as DARPA, with the 'D' standing for Department of Defense

One example of the Internet's rapid growth in technology is how large corporations transfer goods every second on the Internet so that an order is processed in almost real time. Another, more personal example is the use of the automated teller machine (ATM); when customers access their account to obtain cash, they utilize the Internet. As the Internet becomes more popular it also becomes more vulnerable. Security of the confidentiality, integrity and availability[3] of the information is critical. An example of unavailability is when the SQL Slammer worm blocked access to various ATMs in 2003 (Sieberg and Bash 2003).

The Internet serves an important role for many organizations and can be very critical. For example it is often utilized as the technology for first response to emergencies. Large state agencies as well as colleges and universities may be targets for malicious hackers[4] trying to steal important information. Since the growth of the Internet has developed so rapidly, where can public administrators go to gather more information on current threats and trends? The next section discusses the growth of the security portals on the Internet.

B. Information security organizations

The CERT® Coordination Center (CERT/CC) is part of the Software Engineering Institute operated by Carnegie Mellon University for the Department of Defense. CERT/CC, created in 1988, was originally known as Computer Emergency Response Team (CERT 2005). CERT/CC publishes technical documents and provides current

[3] CIA, the information security triad will be discussed in greater detail later in this paper.
[4] Hacker is defined as "a programmer who breaks into computer systems in order to steal or change or destroy information as a form of cyber-terrorism" (http://wordnet.princeton.edu/perl/webwn?s=hacker). It is important to note that other definitions exist for the term "hacker" and they do not consider the term "hacker" to be of malicious intent.

advice to home users as well as businesses and government agencies. CERT/CC analyzes vulnerabilities and malicious code on the Internet and sends email warnings known as advisories to the security community as quick as possible; giving the community time to react before some malicious code is released.[5] The amount of knowledge needed today to hack a computer is enormously less than it was in the 1980s. Starting in the mid 1980s password guessing was a skill used by intruders to get into systems. Although it seems easy, it was quite difficult to do so without the technology like we have today.

Today there are various password cracker/hacker programs readily available online to be downloaded. Malicious amateur hackers can use various hacker websites (like Packet Storm Security's website http://packetstormsecurity.org[6]) and download the computer code to exploit vulnerable software. Software is considered vulnerable when "available [security] patches had not been applied [installed]" (Updegrove and Gordon 2003). In the 1990s, while computers were transmitting data over the internet, the sessions were hijacked by malicious hackers. By the end of the 1990s, graphical user interfaces (GUIs) have been used to break into systems and cause denial of service attacks on important online computers (CERT/CC 2001). Today there are hundreds, if not thousands, of automated scripts that hackers use to launch attacks on the Internet twenty-four hours a day, seven days a week. In September 2005, The State of Texas lost an estimated $224,000 on known security incidents[7] (DIR 2005).

[5] Of these technical documents and presentations the visual aid used to show the attack sophistication vs. intruder technical knowledge is interesting to look at (see Appendix A).
[6] Warning: This website lists exploit code that can ruin computer systems. Responsible research is key, do not download or click on code if you do not understand it.
[7] 108 out of the 250~ state agencies reporting

CERT/CC is an Internet portal that has assisted public administrators in the handling and understanding of information security. Another Internet portal is the SysAdmin, Audit, Network, Security, (known as SANS) Institute, established in 1989 as a cooperative research and education organization that also provides information to public administrators and the security community. Like CERT/CC, SANS publishes technical documents and provides advice, as well as training to government and business users. Today, SANS website, http://www.sans.org, provides information for well over 165,000 professionals, whereas just five years ago, the website was only known to technical/non-managerial staff. The most important aspect of security is awareness (Maiwald and Sieglein 2003) and SANS provides a great glossary of terms used in security and intrusion detection at http://www.sans.org/resources/glossary.php via the SANS website. SANS, as does CERT/CC, provides an email list service where it can send out new vulnerability information about systems as well as advisories and alerts quickly with great efficiency.

CERT/CC and SANS have both evolved since the big high tech boom in the 1990s. CERT/CC defines its purpose as providing the Internet community a single organization that can coordinate responses to security incidents on the Internet (CERT/CC 2001). CERT/CC now provides the Internet community with education and training along with monetary donations for research and development. How is the "Internet community" utilizing these two Internet portals and the vast amount of information? Does this information, free to the world to view and download, provide a problem to public administrators who do not yet understand the technology behind

security? The next section shows how easy hacking is, with or without the large Internet security portals.

C. Today's open Internet and easy access to hacking

A simple Google[8] search on the word "hacking" will get over 5 million hits. After refining the search, or utilizing the advanced search options in the Google search engine, one can see hundreds of companies' websites defaced, or hacked, all online live (See http://www.zone-h.com/en/defacements for an up-to-date list of defaced websites in real-time). A more experienced person, however, can do some simple searches using Google and come up with passwords available online that were inadvertently published on the Internet (Long 2005). A popular site that publishes these mishaps is known as the "Google Hacking Database" (formerly the "Googledorks" database) found on the website http://johnny.ihackstuff.com. On the website http://johnny.ihackstuff.com, one can find a vast amount of information that system administrators and webmasters[9] inadvertently published. Everything from webcams[10] to usernames, passwords, and even credit card numbers can all be found by simple Google searches.

Has CERT/CC and SANS done more harm than good with its technical documentation? Could too much information in the wrong hands cause a disaster? That is debatable and opinions vary on this topic. Although Richard Clarke, former White House Terrorism Advisor, warned of a "digital Pearl Harbor," there are others who disagree. Joshua Green, editor of The Washington Monthly, wrote in 2002, "There is no

[8] Google is a popular Internet search engine that can provide extremely fast results to searches on the Internet. Goggle can be found at www.google.com.
[9] System administrators and webmasters, in this context are those individuals who are responsible for computer systems and online content on websites.
[10] Webcams are security cameras that utilized the internet to transfer the images to a certain console

such thing as cyberterroism—no instance of anyone ever having been killed by a terrorist (or anyone else) using a computer." Green goes on to state, "Nor is there compelling evidence that al Qaeda or any other terrorist organization has resorted to computers for any sort of serious destructive activity."

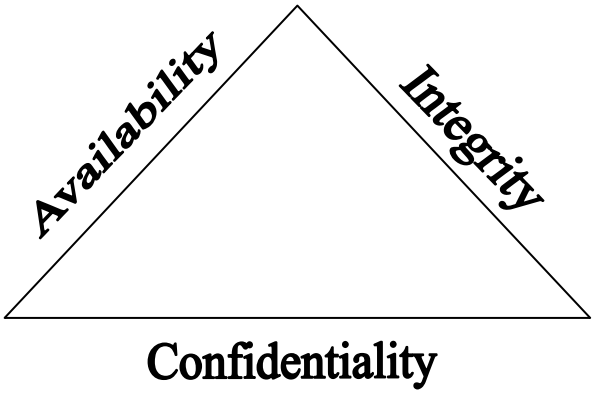
Knowledge is power and CERT/CC along with SANS as internet portals, and http://johnny.ihackstuff.com surely provide a great resource for hackers with malicious intent. CERT/CC and SANS, do however, serve their purpose to the Internet community. Internet communities such as CERT/CC and SANS assist those with a non-technical background understand the importance of computer security. Hackers may use the information published in SANS and CERT/CC to their advantage, but security professionals who keep up with the latest vulnerabilities are a step ahead of hackers because they are able to take various measures to protect their systems in a timely manner.

The internet is continuously growing and with that growth come vulnerabilities. How does a public administrator protect the public's assets and data? What exactly is an information security program and were does one start? The next section describes the components of an ideal security program based on the literature. An information security risk assessment may not be as effective if there is no information security program in place because one has to understand the what, when, and where of the risks that threaten the university and/or agency. Once administrators can understand the risk, then preparations and mitigation can take place to help protect it.

CHAPTER III. AN INFORMATION SECURITY PROGRAM

All security programs start with the CIA triad (Solomon and Chapple 2005; Maiwald and Sieglein 2002; McCumber 2005). The CIA triad is referring to Confidentiality, Integrity and Availability of data (See Figure 3.1). Confidentiality means that the assets of a computing system are accessible only by authorized parties. The type of access is read-type access: reading, viewing, printing, or even just knowing the existence of an object. Confidentiality is sometimes called secrecy or privacy. Integrity means that assets can be modified only by authorized parties or only in authorized ways. In this context, modification includes writing, changing, changing status, deleting, and creating. Availability means that assets are accessible to authorized parties. An authorized party should not be prevented from accessing objects to which he, she, or it has legitimate access needs. For example, a security system could preserve perfect confidentiality by preventing everyone from reading a particular object. However, this system does not meet the requirement of availability for proper access. Availability is known by its opposite, denial of service. Along with the fundamental basis of the CIA triad, a security program must start with the proper policies and must gather input from all the senior leadership of the organization (Maiwald and Sieglein, 2002). To create an information security program it is essential that the Information Security Officer (or Director of the Information Security Office) speak with all the business units, legal department, internal audit, and other key personnel to ensure that everyone is included in the start of this critical piece to the overall organization.

Figure 3.1 – CIA Triad



A. Placement of the Information Security Office

The mistake many organizations and universities make is the placement of the Information Security Office (ISO) under the Chief Information Technology Officer or Information Technology Director. Due to the technical nature of ISO, many times security has already started within the Information Technology (IT) area/division and an impromptu ISO starts up within this area. The challenge then starts when IT itself is investigated for risk, malicious intent, incident and/or any other ISO investigation. Where should the ISO report any improper conduct by IT employees? What if the senior leadership in IT knew of a critical vulnerability in an IT system but did not share this with the head of the agency or company due to risk of embarrassment or even job security? Eric Maiwald and William Sieglein (2002, 7) state that, the placement of the organizations ISO under IT "tends to limit the scope of the department unnecessarily and it often becomes difficult for the ISO to work effectively across the [entire] organization."

Placing the ISO under the internal audit division is also a mistake, although not as common as that of the IT, that many organizations make. The internal audit is supposed

to determine compliance and the ISO is supposed to create policy and assurance; creating policy should not be in the same division with compliance (Maiwald and Sieglein 2002).

Thus the Information Security Office is best positioned directly under the President/CEO or Executive Director (Maiwald and Sieglein 2002). The second most ideal position would be directly under General Counsel/Legal Affairs (Maiwald and Sieglein 2002).

i. ISO Mission Statement

It is important that the ISO mission is written clearly and understood by the staff. The ISO is not the office that is solely responsibly for malicious computer attacks nor does the ISO "guarantee the security of the organization's information or systems" state Maiwald and Sieglein (2002). They go on to suggest that the ISO is there to assist in managing the security risk to information for the entire organization, but that is where the ISO mission stops. The following are examples of mission statement introduced by Maiwald and Sieglein (2002, 8):

- To appropriately manage the information security risk to the organization by working with the various internal departments.
- To appropriately manage the information security risk to the organization by developing and managing organizational security policy.
- To appropriately manage the information security risk to the IT department of the organization by managing the implementation of the organization security policy.

The mission statement, will give the office its direction and provide a solid foundation from which the ISO to work.

ii. The Information Security Office Staff

The ISO staff should have a basic knowledge of networks, different operating systems (OS) (Windows, Unix and Linux, as well as Macintosh), and software development. It is recommended that any security staff be professionally certified. There are many different certifications in the technical world, but few stand out as professional security certifications. First is the Certified Information Systems Security Professional (CISSP) from the International Information Systems Security Certification Consortium which tests the student's knowledge on "the 10 domains of security" (Krutz and Vines 2001). The ten domains are:

- Access Control Systems and Methodology
- Application and Systems Development Security
- Business Continuity Planning and Disaster Recovery Planning
- Cryptography
- Law, Investigation, and Ethics
- Operations Security
- Physical Security
- Security Architecture and Models
- Security Management Practices
- Telecommunications and Networking Security

Another respectable professional certification that is known in the profession is the Certified Information System Auditor (CISA), which is administered by the

Information Systems Audit and Control Association (ISACA). The CISA's purpose is to test a candidate's knowledge, evaluation and application of information security audit principles and practices and technical content areas (ISACA 2005). There are six content areas that the CISA tests on, they are:

- Information Security Audit Process
- IT Governance
- Systems and Infrastructure Life Cycle
- IT Service Delivery and Support
- Protection of Information Assets
- Business Continuity and Disaster Recovery

Most company internal auditors who are the technical, information system auditors would likely be a CISA. For ISO staff the CISA is not as common as the CISSP.

A professional certification is one important qualification to look for in security staff. The staff should not only pass a test and understand the theory behind the ten domains, but they should be able to demonstrate the technical skills and the ability to apply the theory in the real world. Another quality is having presentation and consulting skills that will be needed when speaking and training staff in the organization. The security staff must be competent and able to discuss details of security matters with technical system administrators in order to establish and enforce security policies. If the security staff is incompetent and cannot talk to a system administrator about the TCP/IP stack or various network services, the IT department will quickly lose respect, or worse yet, credibility, for the ISO and an unsuccessful security program will result. The same applies to professional and presentation skills. Internal auditors, as well as external

oversight auditors may not take the security staff serious if they cannot present themselves in a professional manner with senior management or communicate on non-technical, executive-level terms.

Lastly, ensure all potential security staff go through a background check. The data that most security professionals use on a daily basis can easily be abused. Most security breaches are internal, mostly disgruntled employees, but some employees who just do not follow the rules.

B. Security Policy

Baskerville and Siponen (2002, 337) affirm, "There is a wide agreement that good information security policy is the foundation of organizations' information security." Similar to traffic laws, chaos will ensue in the absence of clearly written security policies. When laws are broken, people's lives are in danger. The same goes for information security; policies must be in place and followed or data could be leaked, lost, changed and/or damaged. Maiwald and Sieglein (2002, 58) state, "If you don't have a well-defined information security policy then you are fooling yourself if you think you have security in place." The following are the most basic of policies that all organizations and/or universities should have, at the very least.

i. Acceptable Use Policy

Simply put, the Acceptable Use Policy (AUP) tells the employee what is acceptable and what is not acceptable. Without a basic AUP, companies and agencies have a hard time disciplining an employee who has abused the data of customers and constituents. At a minimum every organization should have at least an Acceptable Use

Policy and Data Classification Guidelines (Maiwald and Sieglein 2002). An example of an employee abusing his/her privilege is that of an employee who is running an internet business on the side, using company networks, computers, printers, etc. The AUP can allow for "incidental use," but should give concrete examples, like using the telephone to schedule a doctor's appointment or a lunch with a family member. Computers and the Internet may be used to check the weather, even when not directly related to one's work; however, computers shall never be used for profit for any individual in a company (i.e. running an internet business off the computer network).

Depending on the laws of the state where the agency is located or operates, some AUP's may differ, however, most AUPs should have similar categories. Maiwald and Sieglein (2002, 62) give an example outline in their book Security Planning & Disaster Recovery:

- Introduction
    - Purpose
    - Scope
    - Roles and Responsibilities
- Compliance
- Acceptable Use of IT Resources
    - Computing Code of Conduct
    - Expectation of Privacy
    - Use of Software
    - Unauthorized Communications Methods
- Information Sensitivity and Classification
- Administrative Security Controls
    - Authorization to Use Company IT Resources
    - Privileged User Authority
    - Account Management
    - Log Review
    - Data Backup and Restoration
    - Incident Response
- Physical and Environmental Controls
    - Facility Access Controls
    - Power
    - Temperature and Humidity Control
- Technical Security Controls
    - User Identification and Authentication
    - Malicious Code Protection
    - Host (Desktop, Workstation, and Server) Security
    - Portable Computing Technology Security
    - Network Security

One of the most critical portions of the example above is the "Information Sensitivity and Classification" or Data Classification. The following section will describe data classification and its importance.

ii. Data Classification

All data and systems should be categorized so employees know how to protect the given data. For example, data classified as public information versus confidential information. This could be informational data like a brochure by an agency or university. Nevertheless, an informational brochure is still data and important to the company so it

must be categorized appropriately. In major contrast to public information would be secret information or personal health information, which should be strictly confidential. The release of such confidential information, either by accident or maliciously, could do severe harm to the company or agency, as well as those persons of which the data described.

Data Classification is the fundamental part of the Standards for Security categorization of Federal Information and Information Systems (2004). In the U.S. Federal Government, data classification is mandated by the Federal Information Processing Standards Publications (FIPS PUB 199) (2004). FIPS 199 defines the three "security objectives" as: 1) Confidentiality, 2) Integrity, and 3) Availability. The CIA triad, which is fundamental to any information security program, is mandated by the Federal Government for all Federal data and systems containing data. FIPS PUB 199 goes on to describe the "potential impact" of the release of this data and asks that agencies rate the data with low, moderate and high (FIPS 2004, 2-3).

Most of the literature relating to information security policy and the Texas Administrative Code do the same; ask that data be rated high, medium, or low in the CIA triad (U.S. General Accounting Office 1999; Stoneburner, Goguen and Feringa 2002; Swanson 1998; Harris 2002; Texas Administrative Code §202; Krutz and Vines 2001). Krutz and Vines (2001) list two different data classification concepts. First are those used in the Federal Government, from the lowest level of sensitive, to the highest (Krutz and Vines 2001, 6-7):

- Unclassified – Information that is neither designated as neither sensitive nor classified.

- Sensitive but Unclassified (SBU) – Information that has been designated as a minor secret, but may not create serious damage if disclosed.
- Confidential – Information that is designated to be of a confidential nature. The unauthorized disclosure of this information could cause some damage to the country's national security.
- Secret – Information that is designated of a secret nature. The unauthorized disclosure of this information could cause serious damage to the country's national security.
- Top Secret – The highest level of information classification (actually the President of the United States has a level only for him). The unauthorized disclosure of Top Secret information will cause exceptionally grave damage to the country's national security.

The other classification concept Krutz and Vines (2001) list is what is used in much of the public sector, again from the lowest level of sensitive to the highest (Krutz and Vines 2001, 7):

- Public – Information that is similar to unclassified information; all of a company's information that does not fit into any of the next categories can be considered public.
- Sensitive – Information that requires a higher level of classification than normal data. This information is protected from a loss of confidentiality, as well as from a loss of integrity due to an unauthorized alteration.

- Private – Information that is considered of a personal nature and is intended for company use only. Its disclosure could adversely affect the company/organization or its employees.
- Confidential – Information that is considered highly sensitive and is intended for internal use only (Maiwald and Sieglein 2002).

For simplicity, it is suggested to keep usage of the CIA triad and high medium and low when categorizing data. Any of the above will work; however, for the purposes of this research, the following is recommended: if in any of the CIA triad a "high" rating is given to data, it is best to protect that data as if it were all "high" and categorize it as the highest (in this case, Category I). The same applies if data is given a "medium" rating and "low" in the rest of the CIA. The U.S. military uses the same paradigm, in that if one small piece of data is confidential on a public machine, then the entire machine is confidential and subject to the high standards of protection for confidential machines.

For a visual/graphical view of how data could be classified or categorized, see figure 1 below.

Figure 1 Data Classification

DATA CLASSIFICATION			
	CATEGORY I	**CATEGORY II**	**CATEGORY III**
NEED FOR CONFIDENTIALITY	HIGH	MEDIUM	LOW
	AND/OR	**AND/OR**	**AND/OR**
NEED FOR INTEGRITY	HIGH	MEDIUM	LOW
	AND/OR	**AND/OR**	**AND/OR**
NEED FOR AVAILABILITY	HIGH	MEDIUM	LOW

Once data and systems are properly classified, the ISO can recommend controls. The three categories of controls are Management, Operational, and Technical Controls (Swanson 2001). It is important that management understand the concepts of these given controls. Bruce Schneier writes (xii 2004), "If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology." Public administrators must understand the classification of data and the risk before they can protect it.

Once the owners properly identify the data and systems that contain data, a risk assessment can be conducted by the ISO. A solid AUP with supporting documents and/or policies, data classification guidelines, and management, operational, and technical controls are all ideal components of an information security plan, as well as ideal components of a security risk assessment done to evaluate the security of an organization.

The following section will give a brief introduction into the federal laws, rules and regulations that companies, public agencies, and higher educational institutions need to be aware of.

CHAPTER IV. LAWS & REGULATIONS ON INFORMATION SECURITY

According to Solomon and Chapple, there's an old saying from the intelligence field, "*In God we trust…All others we monitor*" (2005, 99). Computer security professionals follow this saying and monitor as much data as they possibly can. However, who watches over them? How? For the purposes of this research, the laws are not described in great detail, but are introduced for further research for those who are creating an ISO from the ground up.

There are various laws and/or regulations that ensure proper funding and sufficient staff in the ISO to ensure a secure organization. One of the more recent laws that assist the federal government is the USA PATRIOT Act, enacted in the wake of the September 11 tragedy of 2001 (Solomon and Chapple 2005).

A. The USA PATRIOT Act

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, or the USA PATRIOT Act, passed in the wake of the September 11 tragedy, increased the authority of U.S. law enforcement for the stated purpose of fighting terrorist acts in the United States and abroad. The PATRIOT Act has ten titles; of the ten, the most controversial is Section 215, which allows federal agents to obtain a warrant from a secret federal court for library or bookstore records of anyone connected to an investigation of international terrorism or spying (Egelko 2003).

B. Family Educational Rights and Privacy Act

One of the first privacy laws that went into effect with the constituent/customer in mind was the Family Educational Rights and Privacy Act, known as FERPA. FERPA protects student educational records at universities and other places of education. Miles, et al. (2004) list the types of information that FERPA protects, such as student academic records, student financial records, school finance records (pertaining to the individual student), and other personal, identifiable information of a student.

FERPA, like many of the laws in the following section, are concerned with the confidentiality, integrity and availability of the customer information--in this case student information. The confidentiality, integrity, and availability of information, known as the CIA triad, form the basis of most privacy laws and are fundamental to any information security program (Solomon and Chapple 2005; Harris 2002; Maiwald and Sieglein 2002; Krutz and Vines 2001). The U.S. Health Insurance Portability and Accountability Act (HIPAA) and Gramm-Leach-Bliley Act were also passed in the last few years as the Internet has grown.

C. Health Insurance Portability and Accountability (HIPAA)

HIPAA was signed into law on August 21, 1996, by President Clinton. HIPAA applies not only to hospitals and doctors, but also to anyone who handles Protected Health Information (PHI) (Solomon and Chapple 2005). PHI is handled by researchers and health clinics at universities, as well as human resources divisions within any given company and/or agency. HIPAA deals with a wide set of health policy issues from healthcare reimbursement fraud to access to health insurance and various administrative

tasks associated with healthcare services. As with any information security program, HIPAA is designed to protect the confidentiality, integrity and availability of health information. Maiwald and Sieglein (2005, 33) state that HIPAA sets security standards that are comprised of four areas:

- Administrative procedures
- Physical safeguards
- Technical security services
- Technical security mechanisms

The point of HIPAA is to keep customers' and employees' PHI private, secure, and confidential. The PHI must also be maintained in a manner that ensures high integrity and high availability in the event of an emergency.

D. The Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act (GLB), also known as the Financial Modernization Act of 1999, just like HIPAA targeting those with PHI, targets any company or organization with financial information. Like HIPAA, this law was passed to protect the consumer. According to Solomon and Chapple (2005, 100) GLB proscribes that "those who possess and manipulate private financial information must disclose their uses of that information to the subjects of the records." The Federal Trade Commission's (2005) website states, "These two regulations [Financial Privacy Rule and the Safeguards Rule] apply to 'financial institutions,' which include not only banks, securities firms, and insurance companies, but also companies providing many other types of financial products and services to consumers." As Maiwald and Sieglein report, "many consumers remember getting 'opt-out' instructions in the mail about third party

disclosures by financial institutions; it all started in the summer of 2001 and was the direct result of GLB" (Maiwald and Sieglein 2002, 29).

For information security professionals, one of the act's most important provisions is that the board of directors for a financial organization is now ultimately responsible for security issues and risk management (Harris 2002). The board is also ultimately responsible for ensuring that all employees are trained on information security.

Like HIPAA, the base of this law is to keep customer data private, secure, and confidential. The personal financial information, like PHI, must also be held to high confidentiality, integrity, and availability standards--a reminder of the fundamental CIA triad that all information security programs are based on.

E. Electronic Communications and Privacy Act of 1986

The significance of the Electronic Communications and Privacy Act (ECPA) of 1986 is its inclusion of wiretapping and privacy laws to cover electronic communication (Harris 2002). This regulation was put in place as technology was growing to ensure privacy of electronic communications from wiretapping and/or eavesdropping. Court approval is required to intercept messages transmitted in this manner. The term *intercept* was redefined "to make it clear that it is illegal to intercept the non-voice portion of a wire communication such as the data or digitized portion of a voice communication" (Maiwald and Sieglein 2002, 24). The significance of this act is that no one, including an employer, can eavesdrop on a suspected fraudulent employee. But the Act does allow the employer to monitor if employees are notified in advance or if the employer has reason to believe the company's interests are in jeopardy" (Maiwald and Sieglein 2002, 25).

This is why most if not all companies ask all employees to sign a non-disclosure

form or an acceptable use policy that states that there should be no expectation of privacy on company or agency networks.

There are other, older laws that must be researched before starting an information security program; two important ones are the Computer Security Act of 1987 and the Privacy Act of 1974. The European Union countries have passed some stringent laws as well. If a company is planning on doing business in Europe, it is important to know and understand laws in those countries. All in all, most of these acts deal with the CIA triad of customer, consumer, or constituent data. Information Security is no longer for the computer person who works in the 'network closet'; it is the responsibility of all employees from the senior management to line employees. Computer security should be taken seriously and planned appropriately.

Many of the laws mentioned also call for a business continuity plan and a disaster recovery plan in the event of a major tragedy. Before any disaster recovery plan (DRP) or business continuity plan (BCP) can start, the company or agency must know what assets/systems are the most valuable and the criticality of the systems, and they must prioritize what order the assets must be recovered in the event of a total shutdown of their computers systems and network. BCP/DRP concepts are discussed in a later section of this paper.

If the agency/university is unaware if data is classified or public information, the agency/university will be unable to evaluate risk. Data classification was discussed earlier in this paper. Once the classification of data is understood, a full risk assessment can take place. The following chapter discusses the ideal components of an information security risk assessment.

CHAPTER V. RISK ASSESSMENT IDEAL COMPONENTS

Assume John Doe lives off the coast of Corpus Christi, Texas. Next imagine a major hurricane (category 4) is coming straight to Corpus Christi. Imagine John Doe having only a few days to prepare and evacuate. What would John Doe do? In what order? What would he take/leave behind? These are important questions families must make every year during hurricane season along the US coastline. Would John Doe spend time trying to save the old shed in the back yard that houses the lawn and gardening equipment? Or would John spend most of his time boarding up windows on the main household? What if he has a back sliding door that was cracked or damaged from an incident a few months ago? A crack in a large window that serves as a door is a major vulnerability to the house; high winds may shatter it, causing water to come inside. When a family makes decisions like this, they are evaluating the risk and mitigating it. That is exactly how a public administrator, a CEO of a company, and an information security officer at a large university and/or agency, each along with key personnel, must go about evaluating, protecting, categorizing, and prioritizing their data and the systems that contain the data, including those with the data of their customers and/or constituents. In the information security profession, this is known as performing a risk assessment. A simple definition of a risk assessment is an evaluation of the security plan.

There are four important components to successful security plan. The first is data classification (U.S. General Accounting Office 1999; Stoneburner, Goguen and Feringa 2002; Swanson 1998; Harris 2002; Texas Administrative Code §202; Krutz and Vines 2001; Mitnick 2002), which was discussed in the above section on policies. The second is management controls, concentrating on controls that management is directly

responsible for (Stoneburner, Goguen and Feringa 2002; Swanson 2001; Swanson 1998; Harris 2002; Krutz and Vines 2001; Mitnick 2002; Freeman, Darr, and Neely 1997). The third is operational controls, which are the day-to-day operations of systems and those that a human is most likely to do or act on (Swanson 2001; Swanson 1998; Harris 2002; Krutz and Vines 2001). The fourth is technical controls, which are usually automated computers applying the controls (Swanson 2001; Swanson 1998; Texas Administrative Code §202; Harris 2002; Krutz and Vines 2001).

Data classification was discussed in the earlier section on policies. The following three major sections of this paper will go into detail on management, operational and technical controls as ideal components of an effective information security risk assessment model. After those components are discussed with the appropriate literature, a conceptual framework section will be discussed for an effective information security risk assessment.

A. Management Controls

The ISO's role is to assist in managing the security risk to information for the entire organization, but that's where Maiwald and Sieglein (2002) claim it stops. With policies like those mentioned above, management can now recommend minimum standards and controls. Management controls focus on the management of the IT security system and the management of risk for a system. These controls include techniques and concerns that are normally addressed by management (Swanson 2001, A-5).

i. Risk Management

Risk is the possibility of something adverse happening. Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk. Risk management is the first in the management controls component. Management must be able to evaluate risk within its own domain or division so it can either accept the risk or mitigate it with certain controls. It is important that the ISO understand they do not own the data. The ISO exists to assure the security of the data by consulting with the data owners, usually the respective business units that are the primary users of the data. Some assume the IT group is the owner of all data; this is a common misconception (Solomon and Chapple 2005). IT is usually the custodian ensuring availability, but not necessarily inputting or accessing the data (Harris 2002).

Risk management encompasses many of the following components and subcomponents, but at an executive management level. Another way of thinking of risk management is to think of it as the meta-conceptual framework of a risk assessment; risk management is the bigger picture. A very simple example of physical risk management would be using a sign-in log sheet at the entrance to the data center and locking certain doors (Maiwald and Sieglein 2002, 79). The use of identification badges also assists in risk management so that strangers to the organization cannot walk into a secured area without security clearance.

Senior management must be involved in risk management from the start. Mitnick (2002, 261) argues, "it's important that management demonstrate a strong, personal commitment to the security program – as opposed to management just 'signing off' on another project." It is critical that management knows and understands risk management and that they appropriately apply controls to mitigate the given risk.

ii. Review of Security Controls

Routine evaluations and response to identified vulnerabilities are important elements of managing the risk of a system (Swanson 2001). The review of security controls is important because it keeps management aware of what security controls are being applied to help mitigate risk as a constantly evolving process. Each individual department should evaluate its own systems and apply any given security controls (i.e. consider security at all levels of the software development lifecycle as well as when purchasing software or contracting with a vendor for services; apply security patches in a timely manner, and run technical vulnerability scans on the network). Are routine self-assessments done? Is there an independent review of security controls after a significant change? Vulnerabilities that are not dealt with are a backdoor into production computers. A review of security controls will help with this risk.

iii. Life Cycle Enforcement

Imagine that a car was designed and sold with the gas mileage as the only criteria that the designers considered. Imagine that there was no consideration of safety or comfort or any other features. The car would probably be uncomfortable and possibly unsafe with few, if any, features. That is why security, safety, comfort, and many other

considerations go into the plan from the start. Like the complexity of building a vehicle, software complexity, due to the number and size of interrelated software programs and subprograms, could cause a management nightmare if not properly planned from initiation to disposal (Banker, R and Datar, S and Kemerer, C and Zweig, D 1993).

"Like other aspects of an IT system, security is best managed if planned for throughout the IT system life cycle" (Swanson 2001, A-9). This is best done with the support from senior management. There are many models for the IT system life cycle, but most contain five basic phases: initiation, development/acquisition, implementation, operation/maintenance, and disposal. The ISO is most concerned with assuring security by assessing risk from initiation through disposal. Security should be thought of from the beginning (initiation) of any system. There are five basic phases that make up the life cycle involved in developing any computer system. These shall serve as elements in the evaluation of risk:

- Initiation Phase
- Development/Acquisition Phase
- Implementation Phase
- Operation/Maintenance Phase
- Disposal Phase

iv. Disaster Recovery/Business Continuity Planning

The last critical control listed under management is Disaster Recovery and Business Continuity Planning (DRP/BCP) (Swanson 2001). Laudon and Laudon (2004, 460) describe Disaster Recovery Planning (DRP) as "devising plans for the restoration of computing and communication services after they have been disrupted by an event such

as an earthquake, flood, or terrorist attack." Chapple and Solomon (2005, 89) state three primary goals for DRP:

- Facilitate the rapid establishment of an alternative processing facility should a disaster interrupt operations at the primary production site.
- Provide for the maintenance of operations at that alternate facility for an extended period of time.
- Enable the organization to efficiently transition production operations back to the primary facility after the disaster is resolved.

DRP and BCP are not only valuable, but are mandated by recent security legislation. Under their administrative codes and regulations, many state and local governments require a DRP and BCP.

DRP and BCP is the last of the "management controls" under an ideal information security risk assessment model or information security program. The next section, Operational Controls, is categorized by Swanson (2001) as "addressing security methods focusing on mechanisms primarily implemented and executed by people (as opposed to systems). These controls are put in place to improve the security of a particular system (or group of systems). They often require technical or specialized expertise and often rely upon management activities as well as technical controls."

B. Operational Controls

Operational controls are those that are executed by people and not computers. These could be part of management controls, but normally require more technical skill than most management controls. The operational controls do, however, rely on management for an effective information security program and risk assessment.

The five subcategories under operational controls are personnel security, physical security, documentation, security awareness/training/education, and incident management (Swanson 2001). They are descried in greater detail in the following sections.

i. Personnel Security

Humans perform all computer security programming, policy writing, backups; however, not all employees will need to know certain information. How individuals act and react to computers and the data they have access to is critical to the organization/university. Organizations must be on the alert to the disgruntled employee who tampers with or falsifies data input (Krutz and Vines 2001). Personnel security is defined by Krutz and Vines (2001, 224) as "administrative human resources controls that are used to support the guarantees on the quality levels of personnel performing the computer operations." Krutz and Vines (2001, 224) define administrative controls as "the controls that are installed and maintained by administrative management to help reduce to help reduce the threat or impact of violations on computer security."

Least privilege, background checks, as well as separation of duties, should all be taken into consideration when considering personnel security. The following will describe physical and environmental security.

ii. Physical and Environmental Security

Physical and environmental security is defined by Swanson (2001, A-21) as the measures taken to protect systems, buildings, and related supporting infrastructures against threats associated with their physical environment. Securing information is not just in the digital format; data can be lost by fire and other environmental hazards. Bruce

Schneier rewrote (2004, 27) in his preface to *Secrets and Lies* (1999), "If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology." For the purposes of this research, physical and environmental security has been combined into physical security.

iii. Documentation

Appropriate documentation is critical in various other circumstances in the IT world, including a disaster, unforeseen turnover, or a disgruntled employee. Imagine moving or upgrading an old system to a new one and new employees are unaware what is connected to it and why. Documentation is defined by Laudon and Laudon (2004, 394) as "descriptions of how an information system works from both a technical and/or an end-user standpoint." Undocumented steps of how systems work, technical or not, is always a risk, because although most vendors provide documentation, none can offer the configuration of a system that is imbedded in the network of an organization.

Depending on the networks and systems in any given organization or university, more documentation may be needed that is specific to the organization. ISO staff may need to assist in the security documentation of systems. Maiwald and Sieglein (2002, 114) note that "The security department (specifically the security staff who worked on the project) should develop the portion of the turnover documentation that defines the security mechanisms, how they work, and how they must be operated."

User education can come from good documentation, but it is not the only way. The following section will discuss security awareness and the training and education of users and technical staff.

iv. Security Awareness

Krutz and Vines (2001, 24) describe security awareness as "referring to the general, collective awareness of an organization's personnel of the importance of security and security controls." Security awareness for users is the most cost effective way of reducing risk because if users are aware of the threats they may react to malicious emails, code, webpages and even social engineers with a more security conscious mindset. Many times security awareness is overlooked by ISOs because much of their time is spent on the more technical portion of the job (i.e. monitoring the intrusion detection systems) (Krutz and Vines 2001). Bruce Schneier (2004, 255) writes in *Secrets and Lies*, "People often represent the weakest link in the security chain and are chronically responsible for the failure of security systems." Kevin Mitnick (2003) states that companies are spending millions on security technology, but are ignoring user awareness which bring about the user community as the weakest link.

How users and technical staff handle security incidents is also an important part of an information security program. The following section will discuss incident management.

v. Incident Management

In a perfect world, no security incidents would happen, but the truth is that security incidents occur every day and, depending on the severity, some would say incidents (i.e. network scans) happen just about every second on a large network. "Computer security incidents, according to Swanson, are an adverse event in a computer system or network" (2001, A-40). With automated worms and computer viruses, computer security incidents are happening more rapidly and causing more damage than

ever before. Is there a capability to assist users if a security incident were to occur on their system? Is the information shared with appropriate organizations? These are two critical questions asked by Swanson in her self-assessment survey (2001, A-40-A-41).

If a major security incident were to occur at a large university or state agency, is there appropriate staff ready with an incident response plan? What are the important elements of incident management?

Incident management is the last subcomponent of operation controls. The following section will discuss the final component, the technical controls.

C. Technical Controls

Swanson (2001, A-43) describes technical controls as "focusing on security controls that the computer system executes." Swanson (2001) goes on to state that "the controls can provide automated protection for unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data." Solomon and Chapple (2005, 27) describe technical controls as "object access restriction implementation through the use of software of hardware." Solomon and Chapple also call technical controls as logical. Some people in the IT world may refer to technical controls as ACLs, which stands for "Access Control Lists."

The component of 'technical controls' is fairly short and comprises only three categories: 1) identification and authentication; 2) logical access controls; and 3) audit trails, monitoring and logging. These three sections are described in the following sections.

i. Identification and Authentication

Identification and authentication is part of our every day life. If we visit the bank or an ATM to conduct a financial transaction, it is extremely important that our bank can properly identify us. When retrieving money, it is even more important that we are authenticated to the bank to assure there is no malicious act. Swanson (2001, A-43) defines identification and authentication as "a technical measure that prevents unauthorized people (or unauthorized processes) from entering an IT system." The document goes on to state that "access control usually requires that the system be able to identify and differentiate among users."

The most important security measure occurs after classifying or categorizing data (see Data Classification section above); users who have access to confidential data or top secret information must be properly identified and authenticated. In the case of the data classification concept described above (see Data Classification section above), Category I would be the most restricted, and it is important that this data and information be accessed only by those who have special clearance and that the data be protected by various access control lists.

The next section is the second and last section in the 'technical control' category of the ideal risk assessment and information security plan.

ii. Logical Access Controls

Logical access controls, according to Swanson (2001, A-46), are "the system-based mechanisms used to designate who or what is to have access to a specific system resource and the type of transactions and functions that are permitted." For the purposes of this research, logical access controls are the most technical of the technical controls in

that encryption, firewalls and other automated, technical controls are checked in this category.

The following section will address audit trails, monitoring and logging, the last in the ideal component of technical controls for a security risk assessment and information security plan.

iii. Audit Trails, Monitoring & Logging

Audit trails are the same in digital form as they are in written form. For example, when someone rents a car, the person renting and the renter both sign a written form stating the condition of the car. When the car is returned, the renter can check the written form to ensure there was no major damage. The same goes with logging software, only with logging software their intent is to collect information on the computer systems. Swanson (2001, A-50) describes audit trails as "maintaining a record of system activity by [the] system or application processes and by user activity." Swanson goes on to state that "in conjunction with appropriate tools and procedures, audit trails can provide individual accountability, a means to reconstruct events, detect intrusions, and identify problems." In essence, audit trails can go as far as to "recreate" an event to see what went wrong or to investigate a possible crime or malicious activity by a user.

Krutz and Vines (2001, 235) illustrate audit trails as "an audit (or transaction) trail that enables a security practitioner to trace a transaction's history." Audit trails should, according to Krutz and Vines (2001, 235), record the following:

- The transaction's date and time
- Who processed the transaction
- At which terminal the transaction was processed

- Various security events relating to the transactions

Computer forensic investigators rely upon computer system logs. Therefore, logging software should be turned on to its max, without hindering the computer system, so that all transactions are recorded to ensure proper identification and a speedy investigation in the event of a major computer incident.

CHAPTER VI. CONCEPTUAL FRAMEWORK

The purpose of this paper is to explore the literature on information security in order to identify ideal components of a security program and use this information to develop ideal categories for a risk assessment program for educational institutions as well as state and local government agencies. A conceptual framework was developed from Marianne Swanson's (2001) Security Self-assessment Guide for Information Technology Systems. It was then modified by the information gathered from the literature review so that a security survey could be developed to further gather information on these components.

The information security survey on these ideal components was sent out to a list of information security professionals. The survey asked for the top three elements of each ideal component. The survey responses were compiled and analyzed and serve to both support this research as well as further define the elements within each ideal category of a risk assessment program. Shields and Tajalli (2005, 13) describe a conceptual framework as "helping to organize inquiry into the problem at hand and is not expected to be perfect."

Although there is plenty of literature on information security, information on an effective risk assessment model for universities and public agencies is limited. The original framework for the risk assessment was taken from Swanson (2001) and was modified to provide a guide for public institutions as well as state and local agencies. Although universities may have an information security office, few can assess their risk without a model to go from. Utilizing the security self-assessment guide from Swanson (2001) and modifying the categories so they are not U.S. Federal Government specific

was how the latter portion of the ideal components were acquired. Adding data classification as an ideal component in the beginning is how the entire model came together. Table 6.1 shows the linkage between the ideal components for an effective information security risk assessment model and the literature.

Table 6.1: Conceptual Framework

Ideal Type Components	Source
Data Classification - CIA Triad Confidential Integrity Availability	Solomon and Chapple, 2005 Swanson, 2001 Swanson, 1998 Harris, 2002 Texas Administrative Code § 202.72 Krutz and Vines, 2001 Mitnick, 2002
Management Controls - Risk Management - Review of Security Controls - Life Cycle enforcement - Disaster Recovery/Business Continuity Planning	Solomon and Chapple, 2005 Freeman, Darr, Thomas C, and Neely, 1997 Laudon and Laudon, 2004 Stoneburner, Goguen and Feringa, 2002 Swanson, 2001 Swanson, 1998 Texas Administrative Code § 202.72 U.S. General Accounting Office, 1999
Operational Controls - Personnel Security - Physical Security - Documentation - Security Awareness/Training - Incident Management	Harris, 2002 Krutz and Vines, 2001 Swanson, 2001 Swanson, 1998 Texas Administrative Code § 202.72
Technical Controls - Identification and Authentication - Logical Access Control - Audit Trails, Monitoring & Logging	Harris, 2002 Krutz and Vines, 2001 Swanson, 2001 Swanson, 1998 Texas Administrative Code § 202.72

Earlier it was discussed that a simple definition of a risk assessment is an evaluation of the security plan. There are four important components to successful security plan; these four components are also ideal for an effective information security

risk assessment. The first is "data classification,"[11] which was discussed in the above section on policies. The second is "management controls," concentrating on controls that management is directly responsible for and controls. "Management controls" involve the management of the IT security system and the management of risk for a system[12]. The third is "operational controls," which are the day-to-day operations of systems--those that a human is most likely to do or act on (Swanson 2001; Swanson 1998; Harris 2002; Krutz and Vines 2001). The fourth is "technical controls," which are usually automated computers applying the controls (Swanson 2001; Swanson 1998; Texas Administrative Code §202; Harris 2002; Krutz and Vines 2001).

[11] See for example, Harris 2002; Krutz and Vines 2001; Mitnick 2002; Stoneburner, G and Goguen, A and Feringa, A 2002; Swanson 1998; Texas Administrative Code §202; U.S. General Accounting Office 1999
[12] See for example, Stoneburner, Goguen and Feringa 2002; Swanson 2001; Swanson 1998; Harris 2002; Krutz and Vines 2001; Mitnick 2002; Freeman, Darr, and Neely 1997

CHAPTER VII. METHODOLOGY

This chapter explains the research methodology used in this study to collect the data that will be presented in the final risk assessment model at the conclusion of this paper. Survey research was the primary method of collecting data for this research. Ideal components of an effective risk assessment were identified and an open ended survey on those respective components was sent out to public administrators in the information security profession. The ideal components and sub-components are listed below:

- Data Classification
  - CIA Triad
- Management Controls
  - Risk Management
  - Review of Security Controls
  - Life Cycle Enforcement
  - Disaster Recovery/Business Continuity Planning
- Operational Controls
  - Personnel Security
  - Physical Security
  - Documentation
  - Security Awareness/Training
  - Incident Management
- Technical Controls
  - Identification and Authentication
  - Logical Access Control
  - Audit Trails, Monitoring & Logging

A security survey was sent out to public administrators in the information security profession asking for their opinion on the top three elements of each sub-component (except for the first component, data classification). The survey responses were then

compiled and analyzed, and this data serves to both support this research as well as further define the elements within each ideal category of a risk assessment program. The results chapter will provide the data gathered from the survey while the conclusion will introduce an information security risk assessment model for non-federal public administrators (state and local government, including universities).

A. Risk Assessment Survey

The methodology for this research is the gauging technique. A survey was used to gather input from information security professionals in the field of non-federal public administrators. The professionals were surveyed to find the most important elements of each sub-component from an ideal information security risk assessment model. The results help further define the elements within each ideal category of a risk assessment program so that an ideal information security risk assessment model for state and local governments (including universities) can be fashioned.

Babbie (2004, 243) states, "surveys may be used for descriptive, explanatory and exploratory purposes." For the purposes of this research, a list of ideal components for an information security risk assessment will be described, and then professionals surveyed to list the top three elements of each ideal component. The survey results will be assessed by the researcher and the results will be published in the conclusion of this paper.

i. EDUCAUSE listserve

The first email listserve utilized was the EDUCAUSE security listserve since this document is geared toward those in the non-federal public sector and those in higher

education. EDUCAUSE is a nonprofit association whose mission is to advance higher education by promoting the intelligent use of information technology. The EDUCAUSE website can be found at http://www.educause.edu. The EDUCAUSE security listserve is an open email forum meant for higher education administrators to share information regarding information security.

ii. Texas DIR – IRAP listserve

The second email listserve utilized was the Texas Department of Information Resources (DIR) Information Resources Asset Protection (IRAP) information exchange listserve. The IRAP list is for Texas state employees only (which includes representatives from public institutions of higher education). The IRAP listserve is described on the DIR website as "open communications between subject-matter experts in different State of Texas agencies and universities benefiting all members from a collective wisdom and helping with asset protection programs." The IRAP list is the only listserve that has information security topics openly discussed. The IRAP list information can be found at http://www.dir.texas.gov/IRAPC/subscribe.htm.

B. Risks of Survey Research

There are associated risks to the validity of the research when using survey research. Babbie (2004) points out the importance of "follow-up mailings" to act as reminders and to assist in the encouragement of surveys. In this case a few follow-up emails were sent via the listserve to encourage more participation and a higher response rate. Anonymous mail surveys will be impossible since each email will have a "from"

field as well as data from the email headers.[13] However, no personal/identifiable information will be published in this paper.

For the first ideal component, the respondents were asked to answer yes/no questions to keep the survey from being too confusing in the beginning. The yes/no questions were then followed up by twelve open-ended questions that asked the professional to assess the most important element (in any order) of each respective sub-component.

Only those interested in information security are members of these respective listserves, ensuring the competency of the respondents who answered. The full text of the survey instrument can be found in the Appendix section of this paper. The researcher started with the higher education listserve and after one follow-up email, the researcher tried the second listserve, the IRAP list targeting public administrators in the state of Texas.

The operationalization table (Table 7.1) below links the modes of the research to the conceptual framework.

[13] Email headers are like fingerprints of emails. They tell the user where emails come from via which email server, etc.

Table 7.1: Operationalization Table

Ideal Type Components	Methodology	Survey and Questions	Measurement
Data Classification - CIA Triad Confidential Integrity Availability	▪ Survey of Educause listserve ▪ DIR security listserve	Confidential – Do you think it is important to classify into various levels of confidentiality? Integrity – Do you think it is important to classify into various levels of Integrity? Availability – Do you think it is important to classify into various levels of availability?	YES or NO YES or NO YES or NO
Management Controls - Risk Management - Review of Security Controls - Life Cycle enforcement - Disaster Recovery/Business Continuity Planning	▪ Survey of Educause listserve ▪ DIR security listserve	Risk Mgmt – What are the 3 most important elements of Risk Management? Review of Sec Controls – What are the 3 most important elements of security controls? Life Cycle – What are the 3 most important elements of life cycle enforcement? DR/BCP – What are the 3 most important elements of disaster recovery/business continuity planning?	a. b. c. a. b. c. a. b. c. a. b. c.
Operational Controls - Personnel Security - Physical Security - Documentation - Security Awareness - Incident Management	▪ Survey of Educause listserve ▪ DIR security listserve	Personnel Security – What are the 3 most important elements of personnel security? Physical Security – What are the 3 most important elements of physical security? Documentation – What are the 3 most important elements of documentation? Security Awareness – What are the 3 most important elements of security awareness/training? Incident Mgmt – What are the 3 most important elements of incident management?	a. b. c. a. b. c. a. b. c. a. b. c. a. b. c.
Technical Controls - Identification and Authentication - Logical Access Control - Audit Trails, Monitoring & Logging	▪ Survey of Educause listserve ▪ DIR security listserve	Id & Auth – What are the 3 most important elements of identification and authentication? Log Acc Controls – What are the 3 most important elements of logical access controls? Audit Trails, Monitoring & Logging – What are the 3 most important elements of audit trails, monitoring & logging?	a. b. c. a. b. c. a. b. c.

An information security survey on these ideal components was sent out to a list of information security professionals. The survey asked for each professional's opinion of the top three elements of each ideal component. The survey responses were compiled and analyzed and serve to both support this research as well as further define the elements within each ideal category of a risk assessment program.

CHAPTER VIII. RESULTS

This chapter presents the results of the survey. The results will be discussed in the same order as the survey and the Conceptual Framework (see Table 6.1). Only twenty-two surveys were returned and not all were completely answered. The survey recipients were specifically told that their three responses in each category would not be considered or ranked in any particular order and thus these responses will be considered with equal weight.

A. Data Classification

Data classification is the first of the ideal components. The research found that a majority agreed that data should be classified into the CIA triad. All twenty-two of the professionals surveyed stated that classifying data based on confidentiality was important. The vast majority of the respondents said classifying data based on integrity was important. Although not required, a respondent who disagreed admitted that he was unsure what the researcher meant by integrity. 95% of the information security professionals surveyed stated that the classification of data based on its availability was important.

B. Management Controls

Management controls focus on the management of the IT security system and the management of risk for a system. These controls include techniques and concerns that are normally addressed by management (Swanson 2001, A-5). Risk management is the first of the management controls that was asked in the survey.

i. Risk Management

Risk management was one survey question that all twenty-two respondents answered completely; in fact one respondent gave four answers instead of three, which brought the total sample size to 67. Five categories were created from the more common of responses; the remainders were assigned to the "other" category. The categories and their frequencies are presented in Table 8.1

Table 8.1 – Risk Management Results

Category	Frequency	Percentage
Identify/understand/centralize assets	23	34%
Establish a formal risk assessment	23	34%
Involve senior management for decisions and/or full management support	4	6%
Reoccurring/not a one-time process	3	4%
Understand vulnerabilities & risks	5	7%
Other	9	13%
TOTAL	67	100%

Most of the responses were in the two categories, 'identify/understand/centralize assets' and 'establish a formal risk assessment,' with 34%. It is clear that the information security professionals surveyed agreed that identifying, understanding and centralizing assets are an important element of risk management. Establishing a formal risk assessment also is an important element amongst the security professionals. Identifying the ideal components of a risk assessment shall assist these professionals in establishing a formal risk assessment.

The second sub-component of "management controls" is 'review of security controls.' The results are described in the next section.

ii. Review of Security Controls

The review of security controls is important because it keeps management aware of what security controls are being applied to help mitigate risk as a constantly evolving process. The total number of responses was 59 for this component. Five categories were created from the more common of responses; the remainders were assigned to the "other" category. The categories and their frequencies are presented in Table 8.2.

Table 8.2 – Security Controls Results

Category	Frequency	Percentage
Enforcement/Verifiable/Accountability security controls	17	29%
Measurable/Quantifiable and/or understandable controls	15	25%
Policy and/or Procedures	9	15%
Reoccurring/not a one time process	7	12%
Management involvement and/or support	2	3%
Other	8	15%
TOTAL	59	100%

Enforcement, along with 'verifiable and accountability' were all important elements of security controls, according to the respondents. Security controls must also be measurable, quantifiable and/or understandable in order to be effective. The measurement of these controls appear to be of major importance in the risk to agencies.

The third element of management controls is 'life cycle enforcement.' The results are described in the next subsection.

iii. Life Cycle Enforcement

Like other aspects of an IT system, security is best managed if planned for throughout the IT system life cycle. The different phases described in NIST 800-26 are

the following: Initiation Phase, Development/Acquisition Phase, Implementation Phase, Operation/Maintenance Phase, and the Disposal Phase. The survey gave this definition of 'life cycle enforcement' and asked the professionals what were the three most important elements of 'life cycle enforcement.' The sample size for this component was 56. Five categories were created from the more common of responses; the remainders were assigned to the "other" category. The categories and their frequencies are presented in Table 8.3.

Table 8.3 – Life Cycle Enforcement

Category	Frequency	Percentage
Disposal Phase	7	13%
Development/Acquisition phase	6	11%
Management involvement and/or support	6	11%
Operation/Maintenance Phase	6	11%
Implementation Phase	5	9%
Other	26	46%
TOTAL	56	100%

Of the five categories, no category was significantly more important than any other. It is clear that life cycle enforcement is a complex component and requires future research into its most important elements.

The fourth element of management controls is 'disaster recovery/business continuity planning.' The results are described in the next subsection.

iv. Disaster Recovery/Business Continuity Planning

The last component of "management controls" was 'disaster recovery/business continuity planning,' defined as devising plans for the restoration of computing and communication services after they have been disrupted by an event such as an

earthquake, flood, or terrorist attack. There were 60 responses in this component. Five categories were created from the more common of responses; the remainders were assigned to the "other" category. The results, frequency and percentages of response are presented in Table 8.4.

Table 8.4 – Disaster Recovery/Business Continuity Planning

Category	Frequency	Percentage
Establish a plan with specifics (hardware and software specifics as well as personnel roles)	17	28%
Test the plan (full test as well as partial test)	11	18%
Secure/offsite storage of the plan	8	13%
Management support (both moral and financial)	6	10%
Backups	3	5%
Other	15	25%
TOTAL	60	100%

Disaster recovery and business continuity cannot exist without a plan. This is evident in the responses received by the survey. The category to establish a plan with specific hardware and software, as well as personnel roles, received the highest amount with 28% of the total responses. Testing the plan is also very important, receiving 18% of the responses.

Disaster recovery and business continuity planning was the last subcomponent of management controls for an effective information security risk assessment. The following section is on the operational controls.

C. Operational Controls

Operational controls are those that are executed by people and not computers. These could be part of "management controls," but are normally require more technical skill than most management controls. The operational controls do, however, rely on

management, and they are the third category in our ideal information security program and risk assessment. The five categories are personnel security, physical security, documentation, security awareness/training/education, and incident management (Swanson 2001). The following are the results of each respective subcomponent.

i. Personnel Security

The first component of operational controls was personnel security. The description provided in the survey for 'personnel security' was how individuals act and react to computers and the data they have access to. Organizations must be on the alert to the disgruntled employee who tampers with or falsifies data input. The total number of responses for this component was 66. Five categories were created from the more common of responses; the remainders were assigned to the "other" category. The results, frequency and percentages of response are presented in Table 8.5.

Table 8.5 – Personnel Security

Category	Frequency	Percentage
Training and awareness	16	24%
"Need to know" / least privilege	10	15%
Review of logs (especially for sensitive material)	10	15%
Policy and Procedures	7	11%
Background Checks	3	5%
Other	20	30%
TOTAL	66	100%

24% of the responses mentioned training and/or security awareness as an important element, ironically 'security awareness and training' is a subcomponent of "operational controls." Nevertheless, the lack of training and awareness, specifically in personnel security, seems to be of importance according to the respondents of the survey.

The second sub-component of "operational controls" is 'physical and environmental security.' The results are described in the next section.

ii. Physical and Environmental Security

'Physical and environmental security' was grouped into physical security for the purposes of the security survey. The description given was the measures taken to protect systems, buildings, and related supporting infrastructures against threats associated with their physical environment. 65 was the total of responses from the survey in this component. Five categories were created from the more common of responses; the remainders were assigned to the "other" category. The results, frequency and percentages of response are presented in Table 8.6.

Table 8.6 – Physical Security

Category	Frequency	Percentage
Layered Access (Physical protection) & least privilege	20	31%
Keypads / Badge access / Biometrics	9	14%
Access Control Logs / Audit the logs	6	9%
Training / Awareness	5	8%
Video Cameras	4	6%
Other	21	32%
TOTAL	65	100%

A layered physical access and that of least privilege stood out as the most important element of this subcomponent. According to the information security professionals, layered access and least privilege are important elements and are more important than keypad, badge access, biometrics and access control logs.

The third sub-component of "operational controls" is 'documentation.' The results are described in the next section.

iii. Documentation

Documentation is defined in the survey as descriptions of how an information system works from both a technical and/or an end-user standpoint. 65 was the total of responses from the survey in this component. Five categories were created from the more common of responses; the remainders were assigned to the "other" category. The results, frequency and percentages of response are presented in Table 8.7.

Table 8.7 – Documentation

Category	Frequency	Percentage
Complete / thorough	15	23%
living document / updated frequently / current	14	22%
Easily available	12	18%
Understandable by all / not too technical	8	12%
Training	5	8%
Other	15	23%
TOTAL	65	100%

'Complete and thorough documentation,' as well as documentation that is comprised of 'living documents and updated frequently with current information,' are all important elements of documentation.

The fourth sub-component of "operational controls" is 'security awareness.' The results are described in the next section.

iv. Security Awareness

Security awareness was described as the most cost-effective way of reducing risk because if users are aware of the threats, they may react to malicious emails, malicious code, webpages and even social engineers with a more security conscious mindset. There were a total of sixty-one responses for this component. Five categories were created from the more common of responses; the remainders were assigned to the "other" category. The results, frequency and percentages of response are presented in Table 8.8.

Table 8.8 – Security Awareness

Category	Frequency	Percentage
Mandatory & enforceable training	11	18%
Reoccurring (not just once) w/current information	11	18%
Creative, utilize multimedia	10	16%
Access to security awareness information - reminders (login banners/pens/mugs/etc)	8	13%
Policy driven	5	8%
Other	16	26%
TOTAL	61	100%

According to the information security professionals surveyed, it is important that security awareness training be mandatory and enforceable, as well reoccurring with current information. Many of the respondents also believe that creativity and the utilization of multimedia is important in the subcomponent of security awareness.

The fifth sub-component of "operational controls" is 'incident management.' The results are described in the next section.

v. Incident Management

Incident management is the last component in the "operational controls." The following description was given in the security survey about incident management:

computer security incidents are adverse events in a computer system or network. There were 66 total responses for this component. Five categories were created from the more common of responses; the remainders were assigned to the "other" category. The results, frequency and percentages of response are presented in Table 8.9.

Table 8.9 – Incident Management

Category	Frequency	Percentage
Documented policy & formal procedures	17	26%
Having an Incident Team in place (CIRT) [adequate staff] for timely response	9	14%
Document [incident] what happen/chain of custody	7	11%
Identification/Detection of incident	6	9%
Incident handlers are trained and have authority to conduct response	6	9%
Other	21	32%
TOTAL	66	100%

Information security professionals specifically pointed out policy documentation and formal procedures as an important element in incident management. Having an incident response team in place and adequate staff was also important, although not as important as documented policy and formal procedures.

Incident management is the last component of operational controls. The following section will discuss the results of the survey for the technical controls.

D. Technical Controls

Swanson (2001, A-43) describes technical controls as "focusing on security controls that the computer system executes." Swanson goes on to state that "the controls can provide automated protection for unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data" (2001). Solomon and Chapple (2005, 27) describe technical controls as "object access

restriction implementation through the use of software of hardware." Solomon and Chapple also describe technical controls as logical. Some in the IT world may refer to technical controls as ACLs, which stands for "Access Control Lists."

Technical controls are broken into three subsections, identification and authentication, logical access controls, and audit trails, monitoring and logging. The following subsections will present the results of the security survey.

i. Identification and Authentication

Identification and authentication was described in the survey as a technical measure that prevents unauthorized people (or unauthorized processes) from entering an IT system. There were a total of 64 responses for this component. Five categories were created from the more common of responses; the remainders were assigned to the "other" category. The results, frequency and percentages of response are presented in Table 8.10.

Table 8.10 – Identification and Authentication

Category	Frequency	Percentage
Identifiable/verifiable/unique	12	19%
Strong password and access control lists and/or encryption	11	17%
Policy & formal procedures	10	16%
Audit logs / tracking access	7	11%
Multifactor Identification (2-factor or more)	6	9%
Other	18	28%
TOTAL	64	100%

No element stood out more than the others; however, the top three seemed to be of much importance, according to the information security professionals surveyed. Unique and verifiable identification and authentication are an important element of

identification and authentication. Strong password and access control list and/or encryption were also of much importance.

The second sub-component of "technical controls" is 'logical access controls.' The results are described in the next section.

ii. Logical Access Controls

Logical access controls were described in the security survey as system-based mechanisms used to designate who or what is to have access to a specific system resource and the type of transactions and functions that are permitted. There were fifty-five total responses for this component. Five categories were created from the more common of responses; the remainders were assigned to the "other" category. The results, frequency and percentages of response are presented in Table 8.11.

Table 8.11 – Logical Access Controls

Category	Frequency	Percentage
Audit logs / tracking	11	20%
Policy driven & formal procedures	8	15%
Need to know/least privilege	7	13%
Strong password and access control lists and/or encryption	6	11%
Appropriate access for job	6	11%
Other	17	31%
TOTAL	55	100%

According to the information security professionals surveyed, audit logs and tracking access were important elements of the subcomponent 'logical access controls.' As noted in other subcomponents, policy and formal procedures were also important in this subcomponent. The principle of least privilege and "need to know" were also of importance according to the information security professionals surveyed.

The third sub-component of "technical controls" is 'audit trails, monitoring and logging.' The results are described in the next section.

iii. Audit Trails, Monitoring & Logging

Audit trails, monitoring and logging were described in a short paragraph in the security survey. Audit trails were described as maintaining a record of system activity by the system or application processes and by user activity. Monitoring and logging were considered audit trails; however, they usually contain more detail than just audit trails since they are used for troubleshooting more than a security feature. There were a total of sixty responses for this component. Five categories were created from the more common of responses; the remainders were assigned to the "other" category. The results, frequency and percentages of response are presented in Table 8.12.

Table 8.12 – Audit Trails, Monitoring & Logging

Category	Frequency	Percentage
Logs should log sufficient/relevant info	14	23%
Ensure someone/FTE looks at logs regularly	11	18%
Integrity & security of logs/data	9	15%
Appropriate log storage	6	10%
Policies & formal procedures	4	7%
Other	16	27%
TOTAL	60	100%

According to the information security professionals surveyed, an important element of the subcomponent 'audit trails, monitoring and logging' logs should record sufficient and relevant information. Ensuring a full-time employee actually looks at the logs is also important.

Audit trails, monitoring and logging is the final subcomponent of "technical controls" and the last question asked in the survey. The following will sum up all the results

E. Results Summary

This chapter reported the results of the survey by subcomponent. The following subsections sums up the research by each ideal component, giving a guide for important elements of each component when evaluating risk within a state and/or local government agency (including universities).

i. Data Classification

Information security professionals agree with the federal guidelines and literature that data should be classified into the CIA Triad. Every respondent said classifying data based on confidentiality was important. 82% of the respondents stated that classifying data based on integrity was important, while 95% of the respondents stated it was important to classify data based on availability.

It is clear from the respondents of state and local government, including universities, that the CIA Triad is important and should be utilized when assessing risk to an agency. The following table (Table 8.13) sums up the responses for the first ideal component, "data classifications."

Table 8.13 - Data Classification Summary

Subcomponents	Percentages
Confidentiality	100%
Integrity	82%
Availability	95%

ii. Management Controls

This research shows that when assessing risk based on "management controls," the following elements should be taken into consideration. For the subcomponent of 'risk management,' it is clear that an established formal risk assessment is needed, as well as understanding and identifying all assets of the respective agency. To ensure a low risk in 'security controls,' it is important that the controls are enforceable, verifiable and accountable. Policies and procedures are also important and should be checked when assessing for the risk of security controls. When considering the risk for the 'life cycle enforcement' of systems, all phases seem to be of importance. The disposal phase was mentioned the most by the information security professionals. Many professionals mentioned management involvement and/or support of management on the subcomponent of 'life cycle enforcement.' When evaluating risk on 'disaster recovery/business continuity planning,' it is important to look for an established plan with specifics. Hardware and software specifics should be mentioned, as well as personnel roles in the event of a disaster. Table 8.14 has the summary of the 'management controls.'

Table 8.14 – Management Controls summary

Subcomponents	Elements	Percentages
Risk Management	Identify/understand/centralize assets	34%
	Establish a formal risk assessment	34%
	Involve senior management for decisions and/or full management support	6%
	Reoccurring/not a one time process	4%
	Understand vulnerabilities & risks	7%
	Other	13%
Review of Security Controls	Enforcement/Verifiable/Accountability security controls	29%
	Measurable/Quantifiable and/or understandable controls	25%
	Policy and/or Procedures	15%
	Reoccurring/not a one time process	12%
	Management involvement and/or support	3%
	Other	15%
Life Cycle Enforcement	Disposal Phase	13%
	Development/Acquisition phase	11%
	Management involvement and/or support	11%
	Operation/Maintenance Phase	11%
	Implementation Phase	9%
	Other	46%
Disaster Recovery/Business Continuity Planning	Establish a plan with specifics (hardware and software specifics as well as personnel roles)	28%
	Test the plan (full test as well as partial test)	18%
	Secure/offsite storage of the plan	13%
	Management support (both moral and financial)	10%
	Backups	5%
	Other	25%

iii. Operational Controls

This research shows that when evaluating the risk of 'personnel security,' training and awareness are important elements of this subcomponent. The "need to know" and least privilege rule also are of importance and should be considered when evaluating risk of personnel security. Layered access along with least privilege is of importance when

considering the risk for the subcomponent of 'physical security.' Keypads, badge access, and biometrics are also important when evaluating the risk of 'physical security.'

It is important to consider the completeness of documentation when evaluating risk associated with the subcomponent 'documentation.' Ensuring that the documentation is a living documents, updated frequently and always current may prove to be a challenge, but is nonetheless critical to the associated risk of 'documentation.' When evaluating the risk in the subcomponent 'security awareness,' it is important to check for mandatory and enforceable training. Security awareness is not just a one time course new employees go to, but should be reoccurring and constantly updated with current information.

The final subcomponent in "operational controls" is 'incident management.' When evaluating the risk for 'incident management,' it is important to check for documented policy and formal procedure. Some refer to this as an incident response plan. The incident response plan should be thorough with specific procedures when handling an incident. An incident response plan cannot function without information security analysts, so it is also important to ensure an incident response team be ready and fully staffed in the event of an incident. Some information security professionals called this a CIRT, which stands for Computer Incident Response Team. Documenting what happened and keeping a log for the 'chain of custody' is also very important in this subcomponent when evaluating risk. The following table (Table 8.15) has the summary of the 'operational controls.'

Table 8.15 – Summary of Operational Controls

Subcomponents	Elements	Percentages
Personnel Security	Training and awareness	24%
	"need to know" / least privilege	15%
	Review of logs (especially for sensitive material)	15%
	Policy and Procedures	11%
	Background Checks	5%
	Other	30%
Physical Security	Layered Access (Physical protection) & least privilege	31%
	Keypads / Badge access / Biometrics	14%
	Access Control Logs / Audit the logs	9%
	Training / Awareness	8%
	Video Cameras	6%
	Other	32%
Documentation	Complete / thorough	23%
	living document / updated frequently / current	22%
	Easily available	18%
	Understandable by all / not too technical	12%
	Training	8%
	Other	23%
Security Awareness	Mandatory & enforceable training	18%
	Reoccurring (not just once) w/current information	18%
	Creative, utilize multimedia	16%
	Access to security awareness information - reminders (login banners/pens/mugs/etc)	13%
	Policy driven	8%
	Other	26%
Incident Management	Documented policy & formal procedures	26%
	Having an Incident Team in place (CIRT) [adequate staff] for timely response	14%
	Document [incident] what happen/chain of custody	11%
	Identification/Detection of incident	9%
	Incident handlers are trained and have authority to conduct response	9%
	Other	32%

iv. Technical Controls

This research shows that when evaluation risk occurs in the subcomponent of 'identification and authentication,' it is important to check for verifiable and unique identification methods. Weak passwords and a lack of encryption can cause risk; therefore, it is important to consider the strength of the passwords as well as the strength of the encryption used in the agency. When evaluating risk, it is also important to consider the policies and formal procedures associated with 'identification and authentication'.

The research shows that audit logs and the tracking of controls are important in the subcomponent of 'logical access controls.' These controls should be policy driven, and formal procedures should establish the foundation of the logical access controls. Similar to other subcomponents in an ideal risk assessment, the principle of least privilege is also important. Also, employees should only be given access to information they "need to know" to adequately do their respective job functions.

'Audit trails, monitoring and logging' is in the final subcomponent of "technical controls." When evaluating risk in this respective subcomponent, it is important to check for logs that collect sufficient and relevant information. Logs cannot and should not contain too much information as this makes it difficult for analysts to spot irregularities. And yet, logs must collect enough information to file a criminal case in the court of law (assuming a crime has been committed). It is also important to ensure that a full-time employee look at the logs regularly and does not allow the logs to accumulate to the point where they are impossible to review. Logs should also be checked for integrity and

security because, after all, if logs can be changed by a malicious hacker, what good will these logs serve when collecting evidence?

The following table (Table 8.16) give a summary of the 'technical controls results.'

Table 8.16 – Summary of Technical Controls

Subcomponents	Elements	Percentages
Identification and Authentication	Identifiable/verifiable/unique	19%
	Strong password and access control lists and/or encryption	17%
	Policy & formal procedures	16%
	Audit logs / tracking access	11%
	Multifactor Identification (2-factor or more)	9%
	Other	28%
Logical Access Controls	Audit logs / tracking	20%
	Policy driven & formal procedures	15%
	Need to know/least privilege	13%
	Strong password and access control lists and/or encryption	11%
	Appropriate access for job	11%
	Other	31%
Audit Trails, Monitoring & Logging	Logs should log sufficient/relevant info	23%
	Ensure someone/FTE looks at logs regularly	18%
	Integrity & security of logs/data	15%
	Appropriate log storage	10%
	Policies & formal procedures	7%
	Other	27%

This chapter presented the results of the security survey, the following will conclude this research and gives recommendations for further research.

CHAPTER IX. CONCLUSION

Creating an information security program involves many steps. Once a program is in place, assessing the risk of the given organization is one of the first steps to assure the security of the data and its systems. For public administrators in state and local government, as well as public universities, there is little research on conducting an effective risk assessment.

This research provides an introduction to an information security program and explains some of the laws and regulations that affect information security. Policies fundamental to an organization/university were discussed and the ideal components of a risk assessment were described. This research explored the literature on information security in order to identify ideal components of a security program. This information was used to develop subcomponents of ideal categories for a risk assessment program for educational institutions as well as state and local government agencies. A survey instrument using the ideal components of an information security program was developed and sent out to information security professionals in local and state government (including universities) for their input. The survey responses were compiled and analyzed. The most important elements within each subcomponent of an ideal category for a risk assessment program were presented in the results chapter. The results show the important elements according to the information security professionals which help public administrators create an effective risk assessment program in their respective agency.

One weakness of this research was the amount of data obtained by the security survey. Only 22 responded and not all surveys were complete. Certainly more

respondents would have strengthened this research to develop an ideal information security risk assessment. Nevertheless, this shall not end the exploration of information security and the risks involved in today's 'connected' society. Future research could narrow the open ended questions into multiple choice questions to help get a better idea of the work out in the profession.

Another weakness of this research was the technology used to gather input from the professionals. Rather than using an Adobe Acrobat (pdf) form with a 'submit' button, it is strongly recommended to use a web form and/or a third party so any operating system with a browser can answer the survey. Only computers with the latest Adobe Acrobat Reader software were able to fully read and submit the survey via the Adobe software. Others, specifically those using a Linux operating system, were forced into cutting and pasting the questions and answer into an email and sending them to the researcher as inline text. If further research is to be done and questionnaires/surveys are used, the use of an advanced webpage (or form page) that is compatible across all platforms of computer systems is strongly recommended.

Further research is warranted in the field of information security for public administration. Information security is a new and growing field and the lack of understanding the risks involved with information on the internet can cost a substantial amount of money when resolving a problem. Further research could be conducted on one ideal component whereby a researcher can gather detailed information of each subcomponent. It is important that any new research analyzes the changes that may affect the given ideal component. As technology grows and advances, the scope of this research can change dramatically.

Although there were weakness in this research, the information is still vitally important for public agencies. Technology alone cannot and will not solve the problems of computer security. The latest firewall technology is not all that is needed to protect valuable information resources. Public administrators need to understand the risks of information systems, otherwise hackers and malicious code will continue to rage havoc on public computer systems costing tax payers' money. There is a steep learning curve for non-information technology administrators; however, there is help. Public administrators must utilize the security portals and the information that is out on the Internet to successfully protect their networks and computer systems. Public administrators should also utilized the results of this research to further define a formal risk assessment program in their respective agency.

BIBLIOGRAPHY

Banker, R and Datar, S and Kemerer, C and Zweig, D. 1993. Software complexity and maintenance costs. *Communications of the ACM* V36 (11): 81-94.

Baskerville, R and Siponen, M. 2002. An information security meta-policy for emergent organizations. *Logistics Information Management* V15 (5/6):337-346.

Carnegie Mellon University. 2005. About CERT. CERT/CC. September 2. http://www.cert.org/meet_cert/meetcertcc.html.

CERT/CC (2001, February 16). *CERT Coordination Center site*. Retrieved February 16, 2004, from http://www.cert.org/present/internet-security-trends/sld016.htm

Department of Commerce, United States of America. 2004. Federal Information Processing Standards Publication: Standards for Security Categorization of Federal Information and Information Systems (FIPS PUB) 199. Gaithersburg, MD: National Institute of Standards and Technology.

Egelko, B and Gaura, M. 2003. Libraries post Patriot Act warning: Santa Cruz branches tell patrons that FBI may spy on them. *San Francisco Chronicle*. March 10. http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2003/03/10/MN14634.DTL.

Federal Trade Commission. 2005. "Privacy Initiatives." http://www.ftc.gov/privacy/privacyinitiatives/glbact.html

Feit, Sidnie. 1999. TCP/IP: Architecture, protocols, and implementation with IPv6. New York, NY: McGraw-Hill.

Harris, Shon. 2002. CISSP. Berkeley, CA: McGraw-Hill/Osborne.

ISACA. 2005. 2006 CISA Exam Bulletin of Information. http://www.isaca.org.

Laudon, K and Laudon, J. 2004. Management information systems: Managing the digital firm (8th ed). New Jersey, NJ: Prentice-Hall, Inc.

Long, Johnny. 2005. Google Hacking for Penetration Testers. Rockland, MA:Syngress Publishing, Inc.

Maiwald, E and Sieglein, W. 2002. Security Planning & Disaster Recovery. Berkeley, CA: McGraw-Hill/Osborne.

McCumber, John. 2005. Assessing and Managing Security Risk in IT Systems: A Structured Methodology. New York, NY: Auerbach Publications.

Miles, G and Rogers, R and Fuller, E and Hoagberg, M and Dykstra, T. 2004. Security Assessment: Case Studies for Implementing the NSA IAM. Rockland, MA: Syngress Publishing, Inc.

Mitnick, Kevin D. 2003. Are You the Weak Link? *Harvard Business* Review. V81: 18-20

Mitnick, Kevin D. 2002. The Art of Deception. Indianapolis, IN: Wiley Publishing, Inc.

Pfleeger, Charles P. 1997. Security in Computing. Upper Saddle River, NJ: Prentice Hall

Roberts, Paul. 2005. Malicious Keyloggers Run Rampant on Net. eWeek.com http://www.eweek.com/article2/0,1895,1893515,00.asp

Solomon, M and Chapple, M. 2005. Information Security Illuminated. Sudbury, MA: Jones, and Bartlett Publishers.

Schneier, Bruce. 2003. Beyond Fear: Thinking Sensibly About Security in an Uncertain World. New York, NY: Springer-Verlag.

Schneier, Bruce. 2004. Secrets and Lies: Digital Security in a Networked World. New York, NY: Wiley, John & Sons.

Schneier, Bruce. 1999. Security in the Real World: How to Evaluate Security Technology. *Computer Security Journal* V15:1-14. http://www.schneier.com/essay-031-ft.txt

Shields, P and Tajalli, H. 2005. The Missing Link in Successful Student Scholarship. Paper presented at the annual conference of the National Association of Schools of Public Affairs and Administration, Washington D. C.

Stoneburner, G and Goguen, A and Feringa, A. 2002. Risk Management Guide for Information Technology System. *National Institute of Standards and Technology Special Publication 800-30*. Gaithersburg, MD: National Institute of Standards and Technology.

Swanson, Marianne. 2001. Security Self Assessment Guide for Information Technology Systems. *National Institute of Standards and Technology Special Publication 800-26*. Gaithersburg, MD: National Institute of Standards and Technology.

Texas Department of Information Resources. 2004. Texas Administrative Code. *Texas Secretary of State Website*. http://www.sos.state.tx.us/tac/index.shtml

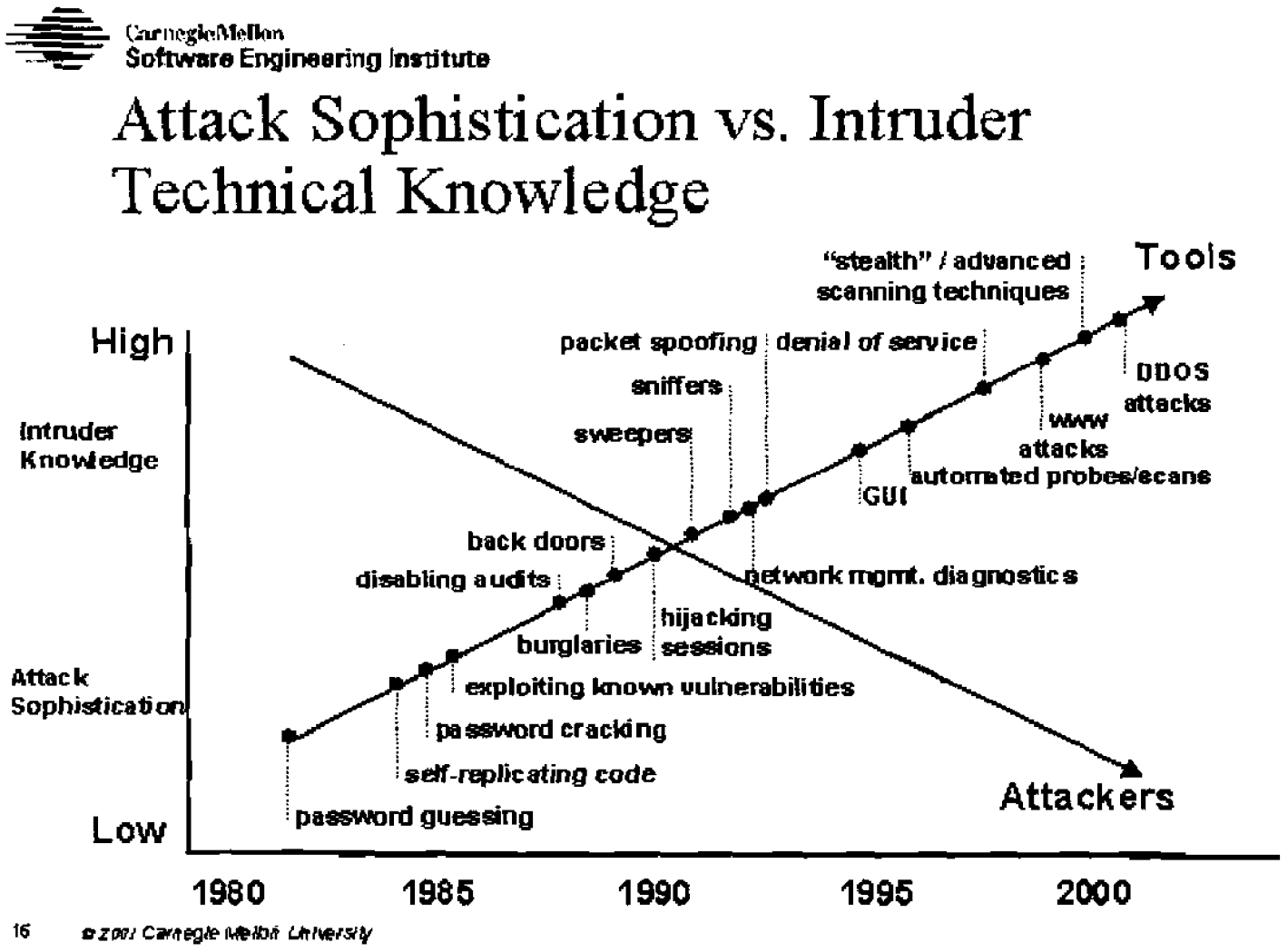
DIR Security Reports. 2005. Monthly Incident Summary Reports: September – November 2005. *Texas Department of Information Resources*. http://www.dir.state.tx.us/security/reports/sepnov05.htm

The SANS Institute. 2003. SANS Glossary of Terms Used in Security and Intrusion Detection. http://www.sans.org/resources/glossary.php

United States General Accounting Office Accounting and Information Management Division. 1999. Federal Information System Controls Audit Manual. http://www.gao.gov/special.pubs/ai12.19.6.pdf

Updegrove, D. and Gordon, W. 2003. Computer and Network Security in Higher Education: Foreword. *Computers and Network Security in Higher Education*, ed. M. Luker and R. Petersen, x-xxii. http://www.educause.edu/ir/library/pdf/pub7008a.pdf

Warman, A.R. 1992. Organizational computer security policy: The reality. *European Journal of Information Systems.* V1 (5):305-310.


Carnegie Mellon
Software Engineering Institute
Attack Sophistication vs. Intruder Technical Knowledge
Tools
"stealth" / advanced scanning techniques
High
Intruder Knowledge
packet spoofing
denial of service
sniffers
sweepers
DDOS attacks
WWW attacks
automated probes/scans
GUI
back doors
disabling audits
network mgmt. diagnostics
hijacking sessions
burglaries
Attack Sophistication
exploiting known vulnerabilities
password cracking
self-replicating code
password guessing
Low
Attackers
1980
1985
1990
1995
2000
16
© 2001 Carnegie Mellon University

APPENDIX B

Email sent to EDUCAUSE and DIR-IRAPC email lists is below:

<start email>
Dear Information Security Professionals:

My name is Victoriano Casas and I am a graduate student at Texas State University (www.txstate.edu) pursuing a Masters in Public Administration (MPA). I also work full time at the University of Texas at Austin as an Information Security Analyst in the Information Security Office. I am currently working on my applied research project (ARP, commonly called a thesis) to fulfill the requirements for my degree. I would like to request your participation in a short survey. The focus of my research is security risk assessments.

This research project is non-funded. The intent of this survey is to obtain expert opinion on categories of an information security risk assessment. The survey will take no longer than 10 minutes.

Your response will be kept confidential and only aggregate statistics will be reported. Your individual expert opinion is requested and will not be construed as a representation of your agency or university. The survey is for research only and will not be used to make comparisons between universities and/or state agencies.

Thank you very much for your time and cooperation. If you have any comments or questions, please feel free to contact me or the professor overseeing the research project. Your response is requested by March 17, 2006.

Thank you for participating in this survey. The survey can be downloaded at the following URL:
https://webspace.utexas.edu/vc243/CasasV_Survey.pdf

If you would like a copy of the finished ARP, please email me. I will share a copy of my entire ARP with those who respond to my survey (as an incentive).

Sincerely,
Victoriano Casas III, CISSP
Graduate Student, Texas State University at San Marcos
vcasas@austin.utexas.edu
(512) 232-9371 (office at UT-Austin)

Oversight Professor:
Hassan Tajalli, Ph.D.
Masters of Public Administration Program
Department of Political Science
Texas State University
San Marcos, TX 78666
(512) 245-2143
tajalli@txstate.edu
<end email>

APPENDIX C

Survey of Ideal Risk Assessment Components

Instructions:

The following document contains a list of ideal type components for a full information security risk assessment. The first three questions pertain to the data classification component. The following twelve questions are opened-ended questions asking for your expert opinion of the respective category. The order of your answers in each category will not be ranked. Please read the brief description of each component and then answer the respective question. There will be a **Submit by Email** button at the bottom of this survey.

Data Classification:

Confidentiality. To prevent unauthorized (intentional or unintentional) disclosure of information. - In your opinion is it important to classify into various levels of confidentiality?
YES or NO

Integrity. To prevent unauthorized (intentional or unintentional) alteration or modification of information. - In your opinion is it important to classify into various levels of Integrity?
YES or NO

Availability. To ensure access to data by authorized users (includes customers as well as employees/students) - In your opinion is it important to classify into various levels of availability?
YES or NO

Risk Management. Risk is the possibility of something adverse happening. Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk.- In your opinion what are the 3 most important elements of Risk Management?

Review of Security Controls. The review of security controls is important because it keeps management aware of what security controls are being applied to help mitigate risk as a constantly evolving process.- In your opinion what are the 3 most important elements of security controls?

Life Cycle Enforcement. Like other aspects of an IT system, security is best managed if planned for throughout the IT system life cycle. The different phases described in NIST 800-26 are the following: Initiation Phase, Development/Acquisition Phase, Implementation Phase, Operation/Maintenance Phase, and the Disposal Phase.- In your opinion what are the 3 most important elements of life cycle enforcement?

Disaster Recovery and Business Continuity Planning. Devising plans for the restoration of computing and communication services after they have been disrupted by an event such as an earthquake, flood, or terrorist attack.- In your opinion what are the 3 most important elements of disaster recovery/business continuity planning?

Personnel Security. How individuals act and react to computers and the data they have access to is critical to the organization/university. Organizations must be on the alert to the disgruntled employee who tampers with or falsifies data input.- In your opinion what are the 3 most important elements of personnel security?

Physical Security. The measures taken to protect systems, buildings, and related supporting infrastructures against threats associated with their physical environment.- In your opinion what are the 3 most important elements of physical security?

Documentation. Descriptions of how an information system works from both a technical and/or an end-user standpoint.- In your opinion what are the 3 most important elements of documentation?

Security Awareness/Training. Security awareness for users is the most cost effective way of reducing risk because if users are aware of the threats they may react to malicious emails, code, webpages and even social engineers with a more security conscious mindset.- In your opinion what are the 3 most important elements of security awareness/training?

Incident Management. Computer security incidents are an adverse event in a computer system or network.- In your opinion what are the 3 most important elements of incident management?

Identification & Authentication. A technical measure that prevents unauthorized people (or unauthorized processes) from entering an IT system.- In your opinion what are the 3 most important elements of identification and authentication?

Logical Access Controls. Logical Access Controls are system-based mechanisms used to designate who or what is to have access to a specific system resource and the type of transactions and functions that are permitted.- In your opinion what are the 3 most important elements of logical access controls?

Audit Trails, Monitoring & Logging. Maintaining a record of system activity by the system or application processes and by user activity are audit trails. Monitoring and logging can also be considered audit trails; however, they usually contain more detail than just audit trails; since they are used for troubleshooting more than a security feature. In your opinion what are the 3 most important elements of audit trails, monitoring & logging?