Cyber Security: Assessing the Effectiveness of Medium Sized Texas Counties to Counter a Cyber Terrorist Attack

By
Willie Gerard Bickham

An Applied Research Project
(Political Science 5397)
Submitted to the Department of Political Science
Southwest Texas State University
In Partial Fulfillment
For the Requirements for the Degree of

Masters of Public Administration

(Summer 2003)

Faculty Approval:

____

____

TABLE OF CONTENTS

ABSTRACT

The utilization of cyber technology in our public and private lives has subsequently increased our vulnerabilities to cyber crime. These vulnerabilities require more current and reliable security systems to protect our expanding cyber technology. Even if federal agencies adopt policies and procedures designed to protect the privacy of sensitive electronic information, that information could still be compromised if the security of the Internet servers, operating systems and software applications involved are inadequate. The rash of hacker attacks, Web page defacement and credit card information being posted on electronic bulletin boards can make many medium-sized Texas counties reluctant to conduct sensitive county transactions involving personal or financial data over the Internet.

Medium-sized Texas counties must also be prepared to defend against cyber terrorism. Cyber terrorism, as defined by the F.B.I., is “the illegitimate use of force or violence against persons or property to intimidate or coerce a government, the civilian population or any segment thereof, in furtherance of political or social objectives through the exploitation of systems deployed by the target” (Overholt and Brenner, 2002). The goal of a cyber-terrorist is to disrupt the efficient and routine function of a community (McClure, 2001). Much of modern life depends on computers and computer networks. For many people, the most visible interaction they have with computers is typing at the keyboard of the computer. But computers and networks are critical for key functions of a county such as managing and operating the electric power grid, dams, water and

wastewater, the air traffic control system, and the financial infrastructure. Cyber terrorist could inflict great harm on any medium-sized Texas county by affecting any of the critical key functions. Because of the possibility of a cyber terrorist attack, it is important that medium-sized Texas counties are prepared.

The purpose of the research is three fold. First, the purpose is to describe a model framework for countering cyber terrorism. The second purpose is to assess security systems of medium-sized Texas counties using the model framework. The final purpose is to make recommendations to improve the security systems of medium-sized Texas counties ability to counter cyber terrorism.

A survey was developed from the conceptual framework and sent to the 30 identified medium-sized Texas counties IT Directors to determine what tools they had in place to counter a cyber terrorist attack. The results gathered from the survey were tabulated into frequency distributions. Frequency distributions are useful in describing and assessing the strengths and weaknesses of the counties security system and processes for countering a cyber terrorist attack.

The findings from this research revealed that all of the counties had some of the defense mechanisms recommended for a cyber security system; however only a couple (2) of the counties had all of the defense mechanisms identified in the model. This leads to the recommendation of each county re-assessing their cyber security needs and existing security systems. Developing a comprehensive cyber security system will:

- Reduce vulnerabilities to a cyber attack.

- Provide for a uniform approach to cyber security protection
- In the event of an attack provide an immediate response plan to minimize damage

When many of theses systems were initially developed, the threat of cyber terrorism was not as evident as it is today. Therefore, the fact that several counties were missing components is not a surprise. Today given the recent evidence of our societies cyber terrorism risk, it is imperative that these counties update their systems.

CHAPTER ONE

INTRODUCTION

Historically, American society has been faced with a variety of threats: cold war, world war, racism, civil war, the great depression, segregation and terrorism. Although many can now be considered “history,” these threats have often received widespread public and media attention while in their “prime.” The emergence of the computer age, however, has brought about change to a familiar and much feared threat. Unfortunately, this new threat has not fully gained the attention of our more informed and educated populace. The new threat is cyber terrorism. Cyber terrorism, as defined by the F.B.I., is “the illegitimate use of force or violence against persons or property to intimidate or coerce a government, the civilian population or any segment thereof, in furtherance of political or social objectives through the exploitation of systems deployed by the target” (Overholt and Brenner, 2002).

The September 11, 2001 attacks on the Pentagon and World Trade Center have left the state of protection of the United States in question. The terrorists who committed the horrific incidents of 9/11 communicated and planned those attacks on the Internet. There is no question that Bin Laden’s regime was out to unlawfully use force and violence to intimidate and coerce the United States Government and civilian population. Why were we not fully prepared, and what acts could follow? In an attempt to discover possible ways that terrorists could strike, the government inadvertently stumbled onto a problem that has plagued this nation for many years, namely the weaknesses in the national security system. An evaluation of national security risks soon revealed that the weakest links were in the computer networks that run the United States infrastructure's critical systems. This has led policy makers to seek ways to combat cyber terrorism by promoting computer and network security in order to prevent cyber terrorist attacks (Overholt and Brenner, 2002).

Imagine these scenarios: Through use of conventional computer technology, a terrorist disrupts the computer communication of major financial institutions, U.S. banks and stock markets. The economy as we know it plummets into an abyss. Using the same technology, the terrorist remotely alters the formulas of the water supply in a county in Texas, inserting dangerous amounts of chemical ingredients into the water supply. Allergic reaction and over-doses afflict and kill thousands. At about the same time, the terrorist remotely alters the pressure in suburban gas supply lines, causing explosions. Some may feel insulated from the attacks described above. Experts in the growing field of cyber terrorism, however, generally agree that these terrorist acts are more than mere Hollywood fantasy. With current technology, cyberterrorists are close to, if not already able, to carry out these terrorist acts.

Computer technology is now a significant part of our private lives, and is pervasive in government (Federal, State & Local) and the private sector. The pervasiveness and power of today's computer technology is mind-boggling. Our utility systems, hospitals, banks, academic organizations, etc. are in some cases controlled, by computers. While on one hand, this technology has resulted in more efficient and time saving outcomes, it also leaves society vulnerable to computer hackers. Hackers exploit computers in ways that are unusual and often illegal, typically with the help of special software programs, which are called hacking tools (Denning, 2002).

There are primarily four types of hacking operations. They are: virtual sit-ins and blockades (where groups or individuals make attempts to generate so much traffic that others cannot use it); automated e-mail bombs (the primary objective is to flood the e-mail server so that it becomes unavailable or is unserviceable); Web hacks and computer break-ins (the defacement of a web site with content/information that is not intended to be there), and; computer viruses and worms (an independent program that replicates itself from machine to machine across network connections, often congesting networks as it spreads). The impact of their invasion could cause major crises -- negatively affecting millions of lives (Denning, 2000).

If medium-sized Texas counties are not prepared for a cyber terrorist attack, the attack could disrupt critical key functions. Some of the critical key functions in a county are managing and operating the electric power grid, dams, water and wastewater, the air traffic control system, and the financial infrastructure. Cyber terrorist could inflict great harm on any medium-sized Texas county by affecting any of the critical key functions. Therefore, it is very important that medium-sized Texas counties are prepared for a cyber terrorist attack.

PURPOSE OF THE RESEARCH

Recognition of our medium-sized Texas counties dependence on cyberspace, as well as the potential damage of terrorism, requires an aggressive and comprehensive approach to security. Therefore, the purpose of the research is three fold. First, the purpose is to describe a model framework for countering cyber terrorism. The second purpose is to assess security systems of medium-sized Texas counties using the model framework. The final purpose is to make recommendations to improve the security systems of medium-sized Texas counties ability to counter cyber terrorism.

CHAPTER SUMMARIES

This applied research project consists of six chapters. The next chapter, Chapter Two, provides an overview with background information on types of cyber terrorism. In addition, International Scope, Cyber Crime, U.S. Preparedness for Cyber Terrorism, and Cyber Security Systems are discussed. Chapter Three builds, defends and describes the ideal or model cyber security system. The scholarly literature used to build the model is discussed. Chapter Four discusses the construction and implementation of the survey as well as sampling issues. The results chapter, Chapter Five, examines the findings of the survey. Each security component is discussed and medium sized Texas counties are assessed to determine how prepared the responding counties were to counter cyber terrorism. Chapter Six concludes the study with a summary of the applied research project and recommendations for future research. The appendices contain reference charts and the survey instruments.

CHAPTER TWO

BACKGROUND

The Purpose of the Background chapter is to provide an overview of cyber terrorism. Cyber terrorism is a growing phenomenon with many existing and developing forms. Topics included in this chapter are Types of Cyber Crime and Cyber Terrorism Acts, International Scope, Cyber Crime, U.S. Preparedness for Cyber Terrorism, and Cyber Security Systems. Throughout this paper cyber crime and cyber terrorism are used interchangeable. Most individuals involved in cyber criminal activity implicitly want the society to survive. Those criminals do not expect to get caught and they want to enjoy the good life. Cyber terrorist on the other hand, have the objective to destroy the system. Cyber terrorism is a larger and different kind of threat. The combination of cyber crime and cyber terrorism enhances the treat so much that action must be taken to secure cyberspace.

Types of Cyber Crime and Cyber Terrorism Acts

Bank threats are the most popular form of cyber crime (Spores and Byers, 1998). Hackers break into a bank system, usually a large corporation, and demand a ransom with a threat to destroy the existing system if their demand is not met within a designated time. This form is popular because of the difficulty the bank encounters in trying to identify the hacker as well as a tendency for the bank to pay the ransom versus attempts to capture the hacker. The threat of hackers could range from logic bombs to electromagnetic pulses and high-emission radio frequency guns to destroy bank files (Sproles and Byars, 1998). The rationale is based on the probability of a major financial loss with public knowledge of such an incidence threatening the safety of individual funds; therefore banks will often comply with the terrorist.

Removal of funds from legitimate accounts to bogus hacker accounts is another type of cyber crime. For example, the "1997 Chaos Computer Club" developed software capable of removing funds from a user's bank account. This group of hackers designed a program via the Internet that was capable of tricking Quicken accounting programs. This software program could be used throughout the world to remove funds from any bank utilizing the Quicken accounting program (Sproles and Byars, 1998).

Publicity can be a type of cyber terrorist act deployed by hackers. The power of affecting a large number of individuals can fuel a terrorist's dysfunctional thinking. This publicity is often seen in Internet efforts to disrupt warfare, such as exploiting "Trojan horse" viruses and network worms. The terrorists are not only attempting to destroy systems, but also brag about their abilities to do so. One of the unfortunate results is that it negatively affects many who may not be the actual target of the terrorist (Sproles and Byars, 1998).

Disinformation is another act of cyber terrorism. Disinformation usually starts as rumors that may start a panic among segments of the public. However, given the millions of individuals utilizing the Internet, the impact can be massive. A recent incident was a rumor that a group was stealing kidneys and selling them over the Internet (Sproles and Byars, 1998). The impact caused a sense of panic for many and brought up ethical concerns with the entire transplant process. One can only imagine the fear in those individuals listed as donors as well as potential recipients wondering if their likelihood of receiving a kidney depended on their financial status. Unfortunately, thousands of individuals were affected by this “disinformation” for a period of time.

Cyber terrorist could target our leaders through “data diddling”. Data diddling involves using the Internet to change data in a system and could involve medical, financial, public (government) and private records. The act could range from stealing or changing a password, to accessing systems controlling life saving medical equipment. Data diddling could result in an invasion of privacy of individuals with the potential for multiple outcomes including financial loss and even death if medical records or equipment are accessed (Sproles and Byars, 1998).

A more extreme form of data diddling is “assassination.” Odd as it sounds, according to Sproles and Byars (1998) there was a case involving a hit on a mob leader in which the leader survived. The assassins accessed medical records and changed a medication dose to a lethal amount resulting in the death of the target within hours. This may seem unreal, but assassination is a real cyber terrorism threat, and the other forms of cyber terrorism briefly discussed above have the power to affect many lives in many different ways. Unfortunately for today’s society, the continued growth of Internet users coupled with the expanding knowledge of hacker’s poses an increasing threat.

Medium-sized Texas counties should be prepared for all of the different types of cyber terrorism acts that could be thrown at them. The types of cyber terrorism acts listed could negatively affect all medium-sized counties in Texas.

International Scope

The technology of the Internet is global with Internet access to millions nation wide. This technology to access and communicate to a large population at low cost is the basis for utilization of the Internet in foreign policy. The technology also leaves the possibility for hackers to utilize the Internet to coerce and influence a large population to the communicator's agenda – cyber terrorism. There is documented history regarding terrorist utilization of the Internet. In 1998 Hizbullah disseminated information to describe attacks on Israeli targets. The result of such global access by all, to include terrorists, has led to numerous policy issues such as "privacy, censorship, Internet governance, cyber crime and information warfare, all of which have a foreign policy dimension" (Denning, 2000).

According to Dorthy Denning, the conflict over Kosovo was the first example of war via the Internet. Government and non-government populace used the Internet to disseminate information, spread propaganda and solicit popular support for their positions (Denning, 2000). Hackers utilized the Internet to voice their objections to both Yugoslav and NATO aggression by disrupting service on government computers and taking over their Web sites. The hacking breakthrough resulted in a disruption of political positions via activists seeking to alter foreign policy. The Internet also impacted military decisions. NATO intentionally did not bomb Internet service providers or shut down satellites. The U.S. State Department, said "Full and open access to the Internet can only help the Serbian people know the ugly truth about the atrocities and crimes against humanity being perpetrated in Kosovo by the Milosevic regime". (Denning, 2000).

The global political power and influence of the Internet has resulted in several countries limiting the access of their population to Internet services. According to Reporter Sans Frontiers, as of 1999 forty-five countries were known to restrict Internet access (Hogan, 2000). The most common method was mandatory subscription to state run Internet service, therefore controlling potentially objectionable sites. Other methods include China's system of blocking access to certain sites considered subversive to the government. Unfortunately, hackers have developed measures to access and communicate information within the government control (Hogan, 2000).

The Internet (Web) has global reach. Friends and foe can use it to manipulate foreign policy. Policy makers when formulating policy strategies must take the power of the Internet into account. The benefits of the Internet include an efficient way to disseminate government policies and agendas both domestically and internationally. This form of open communication between countries can build stronger allies. Unfortunately, cyber terrorists may utilize this same system to corrupt foreign policy.

Cyber Crime

The growth of the Internet, which can be accessed throughout the world, has left it a target for crime - cyber crime. According to Marc Rodgers (1999), prior to the mid 1990's, most cyber crimes were perpetrated by insiders. Since the mid 1990's there has been a shift toward criminal organizations attacking bank institutions and committing wide scale fraud – cyber crime (Rogers, 1999).

Canada is considered as high risk for cyber crime. As an open society with minimal preparedness to secure against cyber crime, Canada is referred to as "hacker heaven" (Toulin, 1999). In fact, according to the *Washington Post*, "major system failures in Canada are comparable to the power outage caused by a winter's ice storm in 1998 that devastated Ontario and Quebec." This comparison was made by the Senate in a report of a range of security concerns that need to be addressed in Canada (Toulin, 1999).

Trojan horses are one of the main tools used by hackers to commit cyber crime. Trojan horses are privacy intrusion programs. Trojan horses are becoming more and more prevalent everyday and are already affecting millions of people all over the world. Different from computer viruses, Trojans do not usually damage files, the silently spy on you (Internet Security Alliance, 2003).

It is not known how many computers in cyberspace are infected with Trojans. What is known however is that their number is significant and it continues to grow. Gartner surveys reveal that online retailers are at least 12 times more likely to be defrauded than government. Government data suggests that cyber crime is the fastest growing type of crime. In its' 1999 Computer

Crime and Security Survey, the FBI acknowledges that 62 percent of corporate respondents reported security breaches in the last 12 months. Price Waterhouse Coopers estimates an average damage due to security breach at approximately $ 256,000 per incident (Internet Security Alliance, 2003).

There may be a systematic under-reporting of cyber crime. Firms experienced a serious loss in consumer confidence post 9/11 and are concerned that reporting cyber crime would further erode their clients' confidence. The decrease in reporting has resulted in a direct decrease in many companies' growth. Hence, there is an incentive to ignore or underreport cyber crime. The ultimate solution to cyber crime is improved security measures.

Cyber crime has the ability to cause enormous damage to a large population through the simple activity of typing on a keyboard. In addition, it can be done in minutes, has a low risk of capture and is low cost. The future terrorism acts will involve a computer vs. any weapon or army. A recent and tragic example was September 11th. It is thought that the terrorists communicated via the Internet and accessed information to formulate their plot to attack the U.S.

This potential impact of cyber crime has influenced the increased interest in computer security. In the next section, U.S. preparedness for Cyber Terrorism is discussed.

U.S. Preparedness for Cyber Terrorism

Cyber crime is already occurring in the United States and the potential for cyber terrorism is real. Recognizing the potential for a cyber terrorist attack on our country has lead to a continued effort of preparedness. Therefore, the challenges of preparedness we face for the development of technological security are enormous and require ongoing efforts, including research.

One of the primary resources for research in the area of technological security is at Dartmouth College. In a statement by the College Director, Michael A. Vatis, before the House Committee on Government Reform Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations on Wednesday, September 26, 2001, steps were recommended to reduce the vulnerability to cyber terrorist attacks:

- Maintaining A High Cyber Alert During the War on Terrorism
- Following "Best Practices" for Computer and Physical Security
- Securing Critical Information Assets
- Employing Ingress and Egress Filtering

In addition to these areas, other recommendations included continued support of Research and Development to improve cyber security (Institute for Security Technology Studies, 2001). The challenges to safeguard our cyber communication continue. The ability of a hacker to access and disrupt confidential information with the simple tools of a computer and Internet access makes achieving the goal of developing reliable security systems crucial for U.S. preparedness. U.S. preparedness includes recognition of the real threat of cyber terrorist, current and developing technological security systems and ongoing research in this area. The next section describes some of the current and developing cyber security systems.

Cyber Security Systems

The need for comprehensive and reliable cyber security systems is a reflection of our technological growth and reliance on cyber communications. Unfortunately, it doesn't appear that comprehensive and reliable cyber security have been attained according to a survey by the Computer Security Institute in 2002, which reported that 90% of the respondents-most large corporations and government agencies-reported computer security breaches in the last twelve months (Green, 2003). Damage can be costly, such as the estimated $9 billion in damage worldwide from the 2000 "Love Bug" Virus (Green, 2002). The most important thing to recognize is the need for ongoing research and technology in developing cyber security systems (Robb, 2002).

Cyber technology has grown in society today. Considering the nature of the Internet to allow access to potential customers also allows access to unwanted cyber criminals, the dilemma about cyber security is understandable. This doesn't mean that individuals, companies or governmental agencies should just accept the potential threat without continued efforts to improve cyber security. In fact, the literature shows the contrary with an increased effort to research and develop more reliable security systems. Some of the researchers felt combining systems and or services were the solution. In her article "The Promise of All-In-One Security", Jennifer Jones researched the trend of companies combining security systems for an expansion of security services. The concept is basic - if one system is effective, then two is more effective. In her research, Ms. Jones identified several vendors who switched to combination security functions from traditional separate devices (Jones, 2002). These vendors include, but are not limited to:

- Cisco
- Crossbeam Systems
- Inktomi
- Netscreen technologies
- Nokia
- Sonic Wall
- Tipping Point Technologies

Paul Vinciguerra also identifies the use of combined system components and services as valuable. Vinciguerra identifies the increased risk of cyber terrorism and recommends components of a cyber security system. The initial phase in development of a network security system is to understand the traffic flow and controls required to limit access (Vinciguerra, 2001). "Network designers implement these controls commonly referred to as Access Control Lists (ACLS) on access routers or firewalls" (Vinciguerra, 2001). Routers fragment packages, while firewalls provide a single place for traffic screening (Vinciguerra, 2001). Independently, these cyber security systems are vulnerable to loopholes, but when combined with other security tools, provide a comprehensive defense against cyber terrorism.

This has lead to development of cyber security systems such as the following:

1. **Security Service Model:** The security service model is a cyber security system with the fundamental task of preventing security breach occurrences. Key components of this system include identification, cryptographic key management, security administration, and system protections (NIST, 2001). In addition to the components that avoid cyber hacking, this system includes a detection and recovery component. The benefit of a Security Service model is the system's ability to prevent security breaches from ever happening via prevention (NIST, 2001).
2. **Global Infrastructure Protection System:** The purpose of global infrastructure protection system is to expand existing systems to recognize new classes of distributed information. The foundation of this system is to maintain information at each node via a hierarchical organization structure (De Capitani di Vimercati, Lincoln, Ricculli and Samarati, 2002). Unlike many other cyber security systems that rely on cryptography for protection, the design of global infrastructure protection systems includes a core anomaly detection language. A key feature of this system is the ability to detect anomalies early, thus eliminating or minimizing damage.
3. **IP (Internet Protocol) Sec.** IP is a layered system designed to secure Internet traffic. The layers are: (1) Authentication Header; (2) Encapsulating Security Payload; (3) Identification of Algorithm(s); and (4) Cryptographic keys. The overall goal of this cyber security system is to provide security services for various types of traffic (Kent and Atkins,

1998). This system does not provide security protection for the entire Internet, only the IP layer. It is, however, an example of current efforts to address and improve cyber security.

4. **Internet Security Systems, Inc. (ISS):** Internet Security Systems, Inc is a well-known Internet security provider. ISS is a world leader in software security and provides critical information protection from ongoing threats and misuse (Executive Summary Internet Risk Summary for September 28 through December 31, 2002). "Services include 24/7 system monitoring, emergency response and access to the x-Force and Internet Security Systems' renowned research and development team (Executive Summary Internet Risk Summary for September 28 through December 31, 2002).

5. **Carnivore Surveillance System:** The FBI introduced the Carnivore system in July of 2000 to address the growing concerns regarding societal risk to cyber terrorism (Dunham, 2002). The Carnivore was designed exclusively to carry out court ordered surveillance of electronic communications, e.g., e-mail (Dunham, 2002 page 544). While the FBI currently utilizes this tool to investigate criminal activity such as child pornography, the spying capabilities of the Carnivore have not been completely researched (Dunham, 2002). This could possibly be a crucial tool to be utilized to investigate possible information warfare by foreign countries.

6. **SPADE:** Spade is a multi-dimensional intrusion detection system that combines existing systems for more comprehensive coverage (Liston, 2003).

7. **Commission of Critical Infrastructure**

   The Commission of Critical Infrastructure was commissioned by President Clinton based on the realization of our survivability dependent on electricity, communications and computers, all of which are potentially accessible by cyber terrorists (Sproles and Byars, 1998). The Commission of Critical Infrastructure recommended that critical security systems be 1) protected by adequate firewalls, 2) be isolated from outside connection, and 3) use best practices for password control and protected action logs (Sproles and Byars, 1998).

8. **Two in Reserve**

   Two in reserve was a proposal introduced by Balzer (2002), which stated that companies should hold their two strongest defenses in reserve. This would leave the decision of when to deploy those two strongest defenses to the companies discretion. Once an attack has been discovered, the defensive response is itself subject to threat by hackers. The two in reserve system is designed to protect a companies' response to a cyber threat. Keeping Two in Reserve is a method to prevent hackers' access to a defense system until it is implemented for their capture.

9. **Over the Horizon (OTH) Radar and Related Capabilities**

   OTH is the development of a network tracking system to identify and track approaching cyber threats, like our current system capable of detecting and tracking approaching bombs and missiles (Just, 2002).

10. **Identification and Tracing**

    Identification and tracing is the development of a system capable of early tracing of cyber crimes in a timely manner to support measures to abort, similar to our strategic nuclear war plan that allows constant monitoring of potential sites.

11. **Tracking and Tapping**

    Tracking and tapping is the development of a system that does surveillance and tracks the whereabouts of individual suspects in the physical world to our cyber world.

12. **Virtual Private Corporation**

    The goal of a Virtual Private Corporation is to protect the privacy of data transmitted over the Internet from within a corporation verses open transmission in potential hostile network environments like Virtual Private Networks. Virtual Private Corporations are temporary corporate communication groups that are created to deal with specific Internet penetration problems. Virtual Private Corporations make it difficult for hackers to identify and target a corporation, hence making the company more secure (Cheng, 2002).

13. Deterrence Through Attacker Identification

The identification of cyber criminals is often difficult. Deterrence through attacker identifications goal is to accurately identify and locate attackers, and develop the evidence to support investigations (Tiren, 2002). This would serve to deter the increased cyber crime by increasing the risk of capture.

The above mentioned cyber security systems and others are steps in preparedness for cyberterrorism. However, these steps are only a beginning. Considering the vulnerability of our country's "nervous system", research and development to improve cyber security are essential (Vatis, 2000). "The ultimate solution, then, lies in developing technology that builds in security from the ground up; security features that render networks more resistant, robust, and resilient in the face of attacks" (ISTS, 2001). This research is vital to our national stability and the government recognizes this need. In 2001 the "White House Office of Science and Technology Policy (OSTP) stated that: The Federal government and the private sector are now making substantial investments in cyber security technologies" (ISTS, 2001). According to Vatis, considering the complex interconnected infrastructures, developing key technologies and analytical methodologies is crucial to protecting information infrastructure (2000).

These cyber security systems and others all have their own variance. However, many share some key cyber security system components. These key components include intrusion detection systems, router security, firewalls, anti-virus software, and password protection. The next chapter, Chapter Three builds, defends and describes the ideal model cyber security system. The scholarly literature used to build the model is discussed.

CHAPTER THREE

CYBER SECURITY MODEL

The purpose of this chapter is to review the literature relevant to cyber security and build an ideal model that can be used to assess cyber security systems in medium-sized Texas counties. The cyber security model is divided into categories that the literature identifies as security defense components to counter a cyber terrorist attack. The major categories of the model are listed in order of assignment. The security defense components are: 1) needs assessment, 2) security policy, 3) system components, 4) system auditing, and 5) incident response plan.

Being a former football player and coach, the model derived from the literature is reminiscent of how a football coach prepares for the football season. Like in the cyber security model, the first thing a coach must do is conduct a needs assessment to identify the weaknesses of the team. Weak areas must be identified and strength must be incorporated into those areas to help the team be strong and prepared for the season. Secondly, a coach must set the foundation and expectations for the team. This is similar to the rationale for computer policies. Policies are the foundation upon which a computer security program can be built. The third area involves selecting components that strengthen the cyber security system's ability to defend against penetration. The coach has to identify the offensive and defensive alignment, positions, key personnel and calls that will provide the best advantage for the team to win. Auditing the system is the fourth component. Auditing a system is essentially an evaluation of the strengths and weaknesses. The data collected from an audit can then be utilized in the formation and/or revision of policies, system components and plans. In football, things may not always work as planned and the coach must check areas for weakness and make changes as necessary. Finally, an incident response plan is needed. Football coaches work long hours developing plans to counter what the opposition may do. They have more than one player at all positions in case someone gets hurt. They work on different strategies to counter what plays the opposing teams may call. These plans are worked on during practice throughout the season to prepare players for instances where these type of situations occur. Both the football coach and the IT Director's of Texas counties need a model or strategy to ensure they are ready for anything the opposition may throw at them.

Since the wake of September 11, 2001, our society has been faced with the realizations of our vulnerabilities. These vulnerabilities, combined with our technological growth, have made our cyber space a key target for possible attack. Changes in our cyber technology include: "(1) computer networks have created extremely complex linkages and interdependences that have never existed before, and (2) the majority of critical infrastructures are outside federal control" (Bennett, 2002 page 1). Therefore, the need to secure our cyber space is crucial to our nation's vital functions. This leads to the need for the development of a reliable and comprehensive cyber security model.

I. Needs Assessment

In order to address any problem, one must first define the problem. The way to go about defining the problem is to conduct a cyber security **needs assessment**. While it may be unreasonable to think that one could build a system that is 100 percent safe from invasion, it is possible to identify primary risks and build systems capable of early detection and eradication or immediate recuperation.

Initial Stage

Needs assessment, as an **initial** step, provides the foundation for identifying vulnerabilities of an existing cyber security system. A vulnerability assessment is one of the strategies used in performing a needs assessment. This tool uses powerful consoles to identify and sort threats by severity, allowing a security officer to quickly see the big picture and take appropriate corrective action (Ellis, 2003).

Vulnerability assessment is defined as the systematic examination of a system to identify those critical infrastructures or related components that may be at risk from an attack and the determination of appropriate procedures that can be implemented to reduce that risk (American National Standard for Telecommunications- Telecom Glossary, 2000). A vulnerability assessment is one of the most important activities to perform on the infrastructure, giving clear insight into the server, router and browser vulnerabilities (Ellis, 2003).

Development Stage

Once the needs are identified, a structured plan needs to be **developed**. It is also wise to consult with security experts in collaboration with system developers for optimal outcomes. Compiling a list of needs identified with brief definitions is key information to discuss with an expert consultant. Fourie (2003) identifies six stages that should be identified when conducting a security system needs assessment. Summaries of his findings are listed below.

Stage 1- Ignorant – "Where the bliss of ignorance causes no discomfort." This is essentially building a system without adequate assessment of site needs and utilizing outdated technology.

Stage 2 – Awake - "Where some catalytic event breaks a core paradigm." This results when an individual gains unauthorized access to programs, making security needs more evident to management.

Stage 3 - Vulnerability Flood - "Knowledge exposes the scale of the problem." This results as the auditing of a system reveals all the system vulnerabilities.

Stage 4 – IDS - "Fighting back." Following identification of system vulnerabilities, administration takes action to address the security needs

Stage 5 – Forensics - "Building in the non-repudiation components for prosecution." –The step of recruiting security experts to help revise a system after the realization of company's vulnerabilities have been identified.

Stage 6 - Practically Secure - "Security-mindedness is pervasive from staff to executive." (Fourie, 2003 pages 2-5)

Suzy Clarke (2002) has also identified information that should be included in a needs assessment. Her study summarized the strengths and weaknesses of a cyber security company (NetEngineers), which was contracted by Telco/SecCompany to provide security for their networks. This company had the essential components of a security system to include "an incident handling policy in place for both internal incidents and incidents on client networks”(Clarke, 2002). The outcome of the SecCompany findings in this study were as follows:

- “Never make assumptions.” Test every theory and produce evidence [such as logs] to prove it.
- Test all “inherited” kit at the beginning of a contract and on an ongoing basis
- Put intrusion detection system alerts into context. Collate as much related/background material [such as firewall logs and rule bases] as possible to build up a “scenario” around the alert.
- Have an incident handling policy in place and know when to enforce it. (Clarke, 2002 page 19).

Selection Stage

The results of the needs assessment should help redefine the security system that the organization already has in place or will help with the **selection** of the new security system. Identifying the needs of a system should influence the essential functions of the **selected** or created cyberspace security system (Ellis, 2003).

The idea of a “universally applicable model of security system is near impossible” (Fourie, 2003). However, the more steps taken to identify needs, review the effectiveness of a system and early detection of any loopholes, improves the overall outcome. As part of the security process, organizations must study and understand threats to their networks (as discussed with the needs assessment), design a security policy tailored to meet these threats, and deploy the appropriate solution. This leads to the next recommendation of implementing a computer security policy.

II. Security Policy

A security policy affects all areas of an organization, and should be created by a collaborative process that involves participation from the IT department, human resources (HR), legal, and the executive business team (Cisco Systems, 2002). The security policy is an ongoing procedure that provides consistent steps required of security systems in an objective procedure with measurable outcomes (Department of Information Resources (DIR), 2002).

Security Policy in Place

Security policies are an important step in the cyber security model and all medium-sized Texas counties should have security **policies in place**. In 2001, the President's Committee of Advisors on Science and Technology (PCAST) called for a national policy mandating cyber security. Both private and government entities are adopting such policies. "The purpose of an information systems security policy is to communicate that information security is a priority to the company and that everyone is responsible - and accountable - for maintaining it" (Blake, 2003).

Since the threat of cyber terrorism has been recognized, government regulatory bodies have begun mandating cyber security policies for the organizations they regulate. For example, in 2001 both the Treasury Department and the Federal Reserve System required financial institutions to develop and execute information security systems (Siegel, Sagalow, and Serritella, 2002).

The Health Insurance Portability and Accountability Act (HIPAA) also mandates policies to govern data privacy and security within the health care industry (Siegel, Sagalow, and Serritella, 2002).

Security Policy Updated Regularly

A security policy is useless if it fails against current threats, or cannot be updated to accommodate changes in technology, or the changing needs of business and government (Department of Information Resources (DIR), 2002). Therefore the need of security policies to be **regularly updated** is essential. Ongoing review of systems should consider "past security-relevant decisions and determine if the decisions were appropriate" (DIR, 2002).

Security Policy Include Organization Responsibilities

Middleton (2003) reviewed the recommended steps developed by professional consultants hired to secure a corporation's network with the development of an official policy with "guiding principles that communicate corporate security objectives" as the initial step. Middleton elaborates on the importance of policy as a mandated guide to the structure of a security system. He recommends the policy include "a discussion of **security responsibilities**, penalties for noncompliance, and classification of information. In addition, it should include procedures for network intrusions, laptop security, and data backup and restoration" (Middleton, 2003).

Agreeing with Middleton, Richard Ginski calls for "an organizational-wide security policy" (2003). He recommends an expert panel to research cyber security and develops a security policy that is to be used as baseline information for cyber security (Ginski, 2003). Ginski (2003) documents information regarding government adoption security policy to be the first step implemented in the development of a cyber security system.

Policy Summary

Policies provide standard objective data that can be utilized for training and guiding individuals employed by that organization. Adopting a security policy should provide system structure and objective data for measurable outcomes. Standards provide system details such as design, implementation steps, software mechanisms, and other specifics in quantitative and qualitative terms (DIR, 2002, pg 2). "Policies provide general instructions, while standards provide specific technical requirements" (DIR, 2002, pg 2). In this paper policies and general instructions are used interchangeably as the basic guidelines for what an organization should include in their cyber security model. The elements of a computer security policy should include:

- A concise policy statement describing the purpose of the document
- A description of the scope of information and resources covered by the policy
- Roles and responsibilities for employees
- Security practices specifying network architecture, third-party connections, remote access, name/password management, intrusion detection, back-up and other requirements
- Acceptable use policy (AUP) for network and Internet access
- Incident response procedures for various threat levels
- Document control factors defining how updates to the security policy will occur (Cisco System, 2002)

Several sources recognized the need for policy development to establish guidelines and continuity in cyber security. Ellis (2003) recognizes the process of assessment and data collection leading to the paramount step of policy development. Similarly, the Institute for Information Infrastructure Protection (2003) recommends a universal acceptance of ongoing cyber security research and governed policies. "Research is needed to determine the actual magnitude of the cyber security problem and enable a better understanding of the relationships between forces that shape information infrastructure protection" (Institute for Information Infrastructure Protection, 2003). This leads to another important step in the cyber security model; the selection of cyber security system components.

III. Cyber Security System Components

Once an organization's needs are identified and policies are written, it is now time to look at your system components and revise those that are vulnerable to a cyber terrorist attack. This part of the model involves the review of information gathered from the needs assessment, looking into what system components will better serve your business, and finally adding those system components that will protect your company from a cyber terrorist attack. Discussion of cyber security system components will be discussed in this section.

Intrusion Detection

"An **intrusion detection** system (IDS) is a computer system (possibly a combination of software and hardware) that attempts to perform intrusion detection" (Kerschbaum, Spafford, and Zamboni, 2002). In order for Texas counties to stay secure in a time of computer vulnerability, intrusion detection is needed. Features of an intrusion detection system include: (1) Identification of Attacker; (2) Identification of Type of Attack; (3) Management Alert System; (4)

Report to Single Console; (5) Track Intruder Destination; (6) Screen and Delete False Positives; and (7) Create Custom Signatures (Ginski, 2003). An Intrusion Detection System's purpose is to provide twenty-four hour; seven days a week (24/7) protection against Network Worm type attacks (Brindley, 2002). "IDS monitor computer network traffic and attempt to identify, alert, and present all anomalous activity to the user" (Farshchi, 2003). All medium-sized Texas counties should have IDS.

Router Security

Routers are "the air traffic controllers of the Internet, ensuring that information, in the form of packets, gets from source to destination" (ISTS, 2001). The enormous amount of communications via routing makes this area highly vulnerable to terrorist attack; therefore the need for secure routing systems is crucial. "Routing operations have not yet seen deliberate disruption from malicious activity, but lack of diversity in router operating systems leaves open the possibility for a massive routing attack" (ISTS, 2001).

Firewall Security

Firewalls are basic components of a cyber security system that controls traffic entering and exiting a system (Sutherland, 2003). "Firewalls examine and control the flow of information and services between a protected sub-network and/or host and the outside world" (Halme& Bauer, 2003 page 4). They essentially filter the network traffic. "The goal of the firewall is to provide efficient and authorized access for users inside the firewall to the outside world, while controlling the access of outside users to protected resources by exporting limited and precisely controlled services" (Halme & Bauer, 2003 page 4). Halme and Bauer (2003) recommend firewall software on separate hardware for optimal performance. A properly configured firewall masks your IP address, making it tougher for hackers to locate your computer. Firewalls are designed to prevent hackers from getting into your programs and files, and must be updated regularly to be effective (Federal Trade Commission, 2002). Types of firewalls include:

- **Packet Filtering Firewall -** Looks at IP addresses to determine if certain traffic should be admitted and it looks at individual packets without considering preceding or succeeding information (scrutinizes least amount of traffic) and can handle largest volume of these listed firewalls.
- **Stateful Inspection Firewall -** Analyzes and scrutinizes information overhead and is more secure then packet filtering firewall.
- **Application Proxy Firewall -** Does what the other two do and limits how protocols can communicate. Application Proxy Firewalls provide better protection against security threats and should provide better protection to medium-sized Texas counties (Ginski, 2003).

Anti-Virus Software Protection

Anti-virus software is a utility that looks for viruses, alerts the user and quarantines any that are found (U.S. Department of Commerce, 2002). Computers today face attacks from various types of malicious software, also called mal-ware. The term mal-ware is used as a generic term for viruses, worms, infected Web sites, and other new threats. Any one level of protection may not detect a given type of attack. It is therefore a good idea to have multiple levels of security. Two such levels are e-mail server-based anti-virus software and network-based anti-virus software. E-mail server-based anti-virus programs are an excellent method of stopping attacks before they get inside a company's network. Network based anti-virus software does a good job of protecting computers from attack after the virus reaches them. It is better to intercept viruses before they reach an end user's computer.

Many anti-virus programs can be set to scan incoming e-mail. They only perform this work after the infected mail has reached the user's e-mail box on the server. This usually causes e-mail disruptions (Huffer, 2002). Robert Clyde (2001) also suggests that anti-virus software run on all desktops, servers and gateways (e-mail and firewall). Most anti-virus solutions detect and remove known mobile code threats in addition to viruses.

In a newspaper article written by Kristi O'Flaherty's (1999), Nolan Clemens, principal of TexSYS RD, said that it's not enough to just install the anti-virus software and forget about it. Steps must be taken to keep the software working against the new viruses hitting the networks everyday. It is critical that a network administrator updates the virus protection programs frequently. It is also essential to keep all anti-virus signature files and engines as current as possible (Clyde, 2001). Industry-accepted anti-virus software programs offer updated versions of the protective programs as well as updates, which can be downloaded from the Internet. Clemens said that it is important to a company's protection to incorporate both the latest versions of the software and update the programs often (O'Flaherty, 2000). It is very important that medium-sized Texas counties also incorporate anti-virus software into their computer security plan.

Password Protection

Password Protection is one of the most popular and easily implemented security devices available to protect networks and data. Passwords are a simple authentication technique in which each password is used repeatedly for a period of time, typically 30, 60 or 90 days, to verify an identity (U.S. Department of Commerce, 2002). A serving computer simply compares the requester's password with a list of authorized users. Often, you must protect passwords within a local network to prevent unauthorized updates or access to sensitive data. On the downside, passwords and the subsequent data are also subject to interception if you send them over the network in the clear or unencrypted (Webb, 2001).

Information security professionals usually refer to a password's ability to withstand threats of unauthorized disclosure, discovery through either trial and error or through deterministic methods and covert reuse as the password's "strength" (Spencer, 1997, p 69). Several factors identified by Dunn, Seltzer and Spencer to provide this strength were:

1. Don't use any part of the user name, full name, address, birthday, and so on.
2. Don't use English or even foreign words.
3. Make sure the password is at least eight characters long.
4. Use different kinds of characters in the password (underlines, asterisks, dashes and so on).
5. Include at least one symbol in the second through sixth character.
6. Use a password that is easy to remember and easy to type.
7. Change the password every thirty days to six weeks.

8. Don’t recycle old passwords or use the same one for several different applications.

Lyde Andrews (2001) also introduces another strength that should be included in password protection - the implementation of account lockout. The account would lockout after someone enters the wrong password a specified number of times. This measure helps prevent brute-force password attacks (Andrews, 2001). It is important that medium sized Texas counties include password protection in their computer security plan.

Once an organization’s needs are identified, policies are written and security system components are identified and established - the foundation for a system is in place. Auditing is the fourth area that belongs in the cyber security model.

IV. System Auditing

Auditing Process in Place

Auditing a security system is a key step in the development of an effective security strategy and should be **included** in all medium-sized Texas counties cyber security model. Given the ongoing change and growth in cyber communications, periodic evaluations of security systems effectiveness is essential in preparedness against cyber crime. Examples of recommended areas to audit in a security system include; (1) Correct directory and file permissions (2) Authorized user access only and (3) allowing only authorized actions (Middleton, 2003).

Audits Done Regularly

Audits are designed to identify flaws and provide recommendations for improvements. Auditing, analyzing and responding to threats should be **ongoing**, full-time commitments. Security devices must be **regularly tested** for functionality, scanned for vulnerabilities and **audited at regularly scheduled** intervals (Ellis, 2003).

To keep on top of the latest attack codes and hacker methods, counties should **regularly update** vulnerability files, including: NIDS signatures, anti-virus signatures, patches and service packs. Most vendors offer free file updates as part of an annual subscription package, so staying on top of the vulnerabilities takes only reasonable effort (Ellis, 2003).

System for Implementing Change

Auditing should be part of the early development phase and continue as an ongoing process to provide information to consider for **revisions** and/or development of future cyber security system models (Fourie, 2002). Auditing a system provides periodic system reviews to identify and repair early loopholes in a system in a consistent and objective manner (Siegel, Sagalow, and Serritella, 2002). Organizational **change** is inevitable and may require policy review and revision when indicated. A regular review of an organization's existing system and mandated policies provides an **ongoing evaluation** of process effectiveness (DIR, 2002).

Data from audits of existing systems provides valuable information for selecting systems for different areas of Internet communication (ISTS, 2001). In addition, the incorporation of an ongoing audit of any system provides an additional source of security in that any loophole can be identified early in the process (ISTS, 2001).

Auditing of systems provide a tool for “risk assessment and developing for appropriate risk mitigation strategies” (McClure, 2001). Vulnerability scanning is one of the most useful defense tactics in your security toolkit to identify important weaknesses on intrusion detection systems, firewalls and routers, but especially on the e-mail, Web, data and e-commerce servers using anti-virus software. These scans determine a device’s vulnerability to worms, viruses, attack code and malicious attackers, and whether effective countermeasures (reconfiguration, patches, service packs) have been applied correctly (Ellis, 2003). Including an auditing system in the infrastructure of a cyberspace security system provides an additional step for system preparedness against cyber terrorism.

The needs assessment, policy development, cyber security components and systems audit collaboratively provide the tools necessary in setting the foundation of a cyber security system. In addition to considering the above features for a recommended cyber security model, a response plan also needs to be developed. This leads to the next step of the cyber security model.

V. Incident Response Plan

Introduction

“Terrorist attacks in the US have forced many organizations to critically reevaluate their **incident response plans**, which includes their business continuity plans and disaster recovery arrangements” (Lam, 2002). The tragedy of September 11 along with the recent technology trends have led to a more widespread awareness of incident response and business continuity issues (Mitchell, 2002). Considering our national security is at risk to cyber attack, the importance of attack preparedness is crucial.

The primary objective of an incident response plan is to enable an organization to survive a disaster and to re-establish normal business operations (Lam, 2002). Disaster recovery involves a series of actions that should be taken in the event of major outages (Mitchell, 2002). Disasters can result from events such as:

- Hacker attacks
- Computer viruses
- Electric power failures
- Underground cable cuts or failures
- Fire, flood, earthquake, and other natural disasters at a facility
- Mistakes in system administration

Business continuity involves insuring that an organization’s critical business process, including those utilizing IT systems, can be maintained in the event of a disaster (Mitchell, 2002). In order to survive disaster, medium-sized

Texas Counties must ensure that critical operations can resume within a reasonable time frame.

Incident Response Plan in Place

Since there is no IT system that is 100 percent fool proof, it is important that medium-sized Texas counties have an **incident response plans in place**. The incident response plan should prepare counties for responding to possible emergencies (Halme & Bauer, 2003). The plan should focus primarily on planning and prevention (Gidh, 2003). The incident response plan should take into account the need to:

- Detect the outages or other disaster effects as quickly as possible
- Notify any affected parties so that the can take immediate action
- Isolate the affected systems so that damage cannot spread
- Repair the critical affected systems so that operations can be resumed as quickly as possible

A good incident response plan should include two main IT components of operations: 1) data, and 2) system (Mitchell, 2002). Medium-sized Texas counties should rely on some form of redundancy to make the recovery of data and systems possible. Redundancy allows secondary data or system resources to be pressed into service on short notice should primary resources fail or otherwise become unavailable (Mitchell, 2002). One way to reproduce secondary data is through system backup. System backup controls should be put in place to restore data in the event of an emergency. Backups should be made regularly and should be stored off-site to prevent loss or damage (Lam, 2002). Another approach is disk mirroring. Disk mirroring ensures that data remain available from multiple sources in near real-time. One of the most resent trends in disaster recovery planning is a third-party relocation service. A Third-party relocation service gives organizations access to fully equipped operation space at temporary facilities in remote locations (Mitchell, 2002).

Incident Response Plan Tested

In order to insure the effectiveness of the incident response plan that the counties have adopted, the **plan must be tested**. The incident response plan should be tested to assure minimal damage during emergencies. Incident response plans that look great on paper but are technically unproven will likely fail in practice (Mitchell, 2002).

Incident Response Plan Examined

Due to the ongoing change in technology, once plans are developed and initial test of the plans are conducted, it is important to **reexamine the plan** and make necessary modifications to the plans based on an analysis of the test results. Modifications of the plans are critical to the success of an actual recovery. The modifications should reflect changes to the environments that are supported by the plans (Gidh, 2003).

CONCEPTUAL FRAMEWORK

The conceptual framework for this research is the practical ideal type. The literature supports the existence of a practical ideal type cyber security model. The cyber security components were developed from the literature with its foundation adopted from various sources. To reiterate, the ideal cyber security model consists of 1) needs assessment, 2) security policy, 3) system components, 4) system auditing, and 5) incident response plan. The ideal type categories are organized to follow a logical sequence as summarized below:

Computer Security Needs Assessment

The first step in development of a cyber security system is conducting a needs assessment. The needs assessments main purpose is to identify vulnerabilities within an existing security system. The needs assessment will help IT personnel see the big picture so that they can take proactive measures to correct any problems. Identifying the needs of a cyber security system should influence essential functions of the selected or created cyberspace security system.

Computer Security Policy

The second step in development of a cyber security system requires standard guidelines to follow, such as a security policy. "Policies are management instructions indicating a course of action, a guiding principle, or an appropriate procedure that is expedient, prudent, or advantageous" (Department of Information Resources (DIR), 2002).

Cyber Security System Components

Ideal components of a cyber security system that should provide protection from a cyber terrorism attack include Intrusion Detection Systems, Router Security, Firewalls, Anti-Virus Software and Password Protection.

1. Intrusion Detection Systems

An Intrusion Detection System's purpose is to provide twenty-four hours seven days a week (24/7) protection against Network Worm type attacks (Brindley, 2002). Routers and firewalls, both essential components of a cyber security system, can be categorized as intrusion detection systems. Routers and firewalls have independent functions of routing information and blocking access are incorporated methods for providing in-built intrusion detection and alerting capabilities (Brindley, 2002).

2. Router Security Protection

Routers are "the air traffic controllers of the Internet, ensuring that information, in the form of packets, gets from source to destination" (ISTS, 2001). Routers can mitigate denial-of-service attacks by limiting the bandwidth available to each type of application, thus making bandwidth unavailable to attackers.

3. Firewall Protection

"Firewalls examine and control the flow of information and services between a protected sub-network and/or host and the outside world" (Halme & Bauer, 2003). The goal of the firewall is to provide efficient and authorized access for users "inside" the firewall to the outside world, while controlling the access of “outside” users to protected resources by exporting limited and precisely controlled services (Halme & Bauer, 2003).

4. Anti-Virus Software Protection

Anti-virus software should be implemented by all organizations, considering the growing trend of viruses, worms, and Trojan horses. Anti-virus software should be regularly updated to meet organizations security needs (Cisco Systems, 2002). Norton and McAfee are example of anti–virus software utilized by many personal computer users.

5. Password Protection

“One of the most common ways intruders get access into the network is through exploiting existing user accounts along with their associated passwords” (Andrews, 2001, pg3). Password protection is a crucial step of a comprehensive security system. Password protection should be mandated to all users with clear policy guidelines written for employees to review. Password protection includes, frequently changing the password, avoiding the use of personal information such as names or dates of birth, and avoiding the use of passwords containing letters only. Enforcing strong password policies can significantly reduce the chance of intruders gaining access to a network (Andrews, 2001).

System Auditing

Auditing a system on a regular basis provides information about ongoing network activities both authorized and unauthorized. Auditing provides file information such as creation/deletion, failed login attempts, notification of users attempts to access prohibited directories, etc. (Andrews, 2001). In order to be effective, regular scheduled reviews of auditing logs should be required.

Incident Response Plan

The goal of a incident recovery plan is to identify weaknesses and implement a disaster prevention program, minimize the duration of a serious disruption to business operations, facilitate effective coordination of recovery tasks, and most importantly reduce complexity of the recovery effort (Gidh, 2003).

These security components alone may not be able to survive a terrorist attack on any of the medium-sized Texas counties computer systems, but coupled together should produce positive results. These components should be used to help medium-sized Texas counties begin to identify and fix some of the glaring (i.e. most easily compromised) security holes in their systems and also help the counties be abreast of what to do if penetration into the system occurs.

Table 3.1 links the conceptual framework, the model components and the literature. Each component is identified and separated. Each component has several supporting elements that help validate its existence. The elements validate the use of a needs assessment, security policy, computer security system protection components, system auditing, and an incident response plan.

Table 3.1: Linking the Practical Ideal Components to the Literature, Conceptual Framework

Category and Ideal Type Components	Source
Security Systems Needs Assessment • Initial Stage • Development Stage • Selection Stage	Bennett, 2002 Fourie, 2003 Ellis, 2003 Telcom Glossary, 2000 Clarke, 2002
Security Policy • Policy in place • Policy updated regularly • Include responsibilities of both the organization and its employees	Blake, 2003 Dedge, 2001 Denning, 2000 DIR, 2002 Cisco Systems, 2002 Siegel, Sagalow, Serritella, 2002 Middleton, 2003 Ginski, 2003 Information for Information Infrastructure Protection, 2003 National Strategy to Secure Cyberspace, 2003 Bennett, 2002
Cyber Security System Protection Components • Intrusion Detection Systems Protection • Router Security Protection • Firewalls Protection • Anti-Virus Protection • Password Protection	Brindley, 2002 Halme & Bauer, 2003 Ginski, 2003 ISTS, 2001 Farschchi, 2003 Federal Trade Commission, 2002 Liston, 2003 Vinciguerra, 2001 O'Flaherty, 1999 Huffer, 2002 Clyde, 2001 Dunn, 2002 Poore, 1997 Seltzer, 2002 Webb, 2001 U.S. Department of Commerce, 2002 Spencer, 1997 Andrews, 2001 Kerschbaum, Spafford, & Zamboni, 2002
System Auditing • Auditing process in place • Audits done regularly • System for implementing change	Siegl, Sagalo, & Serritlla, 2002 McClure, 2001 Middelton, 2003 Flourie, 2002 Ellis, 2003 DIR, 2002 ISTS, 2002
Incident Response Plan • Incident plan in place • Plan tested • Plan examined	Halme & Bauer, 2003 Lam, 2002 Balzer, 2002 West-Brown, 2003 Neeley, 2003 Farshch, 2003 Liston, 2003 Gidh, 2003 Mitchell, 2002

CHAPTER FOUR

METHODOLOGY

Purpose

The purpose of this chapter is to describe the methodology used to assess how prepared medium-sized Texas counties are for a possible cyber terrorist attack. The assessment is based on the model (Practical Ideal Type) developed in Chapter Three. The assessment mechanisms should indicate how close anti-cyber terrorism mechanisms are to an ideal established through the literature review.

Introduction to Methodology

Survey research was the method of data collection used to assess the preparedness of medium-sized counties in Texas to a cyber terrorist attack. The survey was based on the model cyber security components (practical ideal type) developed in chapter three. The survey instrument developed for the assessment was constructed from the conceptual framework. In order to address the research purpose, this tool was the most appropriate methodology.

Data Collection Method

Survey research was used to gather data from 30 medium-sized Texas counties. According to Babbie, survey research is the most appropriate research method available to the social researcher who is interested in collecting original data for describing a population too large to observe directly. Surveys are also excellent vehicles for measuring attitudes and orientations in a large population. The use of a questionnaire to conduct survey research is the most appropriate method to use when time and money constraints, and sensitive subject nature, are a consideration (Babbie, 2001, p 238-258).

Though this form of research is faster and more cost effective, it does have its weaknesses. Some of the weaknesses of survey research discussed by Babbie were 1). Response Rate: Without someone there to make the respondent complete the survey, there is a lack of impetus to bother with the study at all. 2). Survey research is generally considered to be weak on validity but strong on reliability. This is due to the fact that responses are limited to particular categories that make observations more artificial. However, these same structured response categories that may promote artificiality also promote reliability due to the fact that all respondents are provided with the same information (Babbie, 2001, p 238-258).

To deal with some of these inherent weaknesses, certain techniques were employed to collect the data. First, to encourage a higher response rate, responses have been structured into simple “yes” or “no” categories (DICHOTOMOUS ITEMS), since the ultimate aim is to determine whether or not particular cyber security components are being used. According to Babbie (2001, p 238-258), if a questionnaire is simple it more likely to be answered.

Secondly, surveys were mailed along with self-addressed stamped envelopes to the Directors of Information Technology (IT Directors) of the 30 identified medium-sized counties in Texas. The survey was pre-tested with IT personnel within the City of Austin. The surveys were mailed on May 16, 2003 with follow up surveys sent to non-respondents on May 28, 2003. Further, phone calls were made on June 16, 2003 to all counties that did not respond. Thirteen (13) counties returned the surveys, making for a 43% response rate. According to Babbie (2001, p. 238-258) a response rate of at least 50% is "adequate for analysis and reporting." If the response rate is lower than 50%, there is a possibility of response bias, where samples taken are not representative of the total population (Babbie, 2001, p. 238-258). However, a response rate of 43% should still be considered a fairly decent rate of return, especially in light of the sensitive nature of the present subject matter. Table 4.1 demonstrates the linking of the survey instrument to the conceptual framework. The table lists each component of the conceptual framework. The table the lists the corresponding survey questions for those components.

Table 4.1: Linking the survey to the Conceptual Framework

Category and Ideal Type Components	Survey Question (yes/no) responses were used
Security Systems Needs Assessment • Initial Stage • Development Stage • Selection Stage	1. Has the county conducted a computer security needs assessment? 2. Was the needs assessment done prior to development of a security policy? 3. Did the needs assessment influence the essential functions of the selected or created security system?
Security Policy • Policy in place • Policy updated regularly • Include responsibilities of both the organization and its employees	4. Are there written policies in place for computer security? 5. Is the security policy updated on a regular basis to stay current with county security needs? 6. Does the security policies include a discussion of security responsibilities? 7. Do the security policies include procedures for noncompliance? 8. Do the security policies include procedures for network intrusion? 9. Do the security policies include procedures for computer backup? 10. Do the security policies include procedures for restoration and classification of information?
Cyber Security System Protection Components • Intrusion Detection Systems Protection • Router Security Protection • Firewalls Protection • Anti-Virus Software Protection • Password Protection	11. Are intrusion detection system utilized? 12. Does the intrusion detection system provide 24/7 Protection? 13. Does the intrusion detection system identify, alert and present all anomalous activity? 14. Does the intrusion detection system provide misuse detection? 15. Does the intrusion detection system also have router security included in it? 16. Does the county use firewalls? 17. Do the firewalls control traffic entering and exiting a system? 18. Are packet filtering firewalls used? 19. Are stateful inspection firewalls used? 20. Are application proxy firewalls used? 21. Does the county use anti-virus software? 22. Does the anti-virus software automatically update its antidotes? 23. Is the anti-virus software run daily, weekly, monthly, annually, never? 24. Does the county use password protection? 25. Are passwords changed every thirty days, sixty days, ninety days, or seldom changed? 26. Are users instructed to use upper case letters, lower case letters, numbers, and signs in there passwords?
System Auditing • Auditing process in place • Audits done regularly • System for implementing change	27. Is there a system auditing process in place? 28. If yes, are the audits performed on regular schedule intervals? 29. If revisions are indicated, do you have a system in place to implement change?
Incident Response Plan • Incident plan in place • Plan tested • Plan examined	30. Is there a computer incident response plan in place? 31. If yes, has the system been tested in a county drill or emergency situation? 32. Is the program examined and modified to ensure its effectiveness against newly defined security threats.

Sample

The sample consisted of thirty medium-sized counties within the state of Texas, ranging in population from 100,000 to 700,000. The sampling frame was taken from the U.S. Census Bureau for Texas County Population Estimates and Population Change: July 1, 2001 to July 1, 2002. There were 30 counties, which have been identified as medium-sized Texas counties. The 30 counties constitute what are considered to be, by this study, medium-sized counties within the state of Texas. The total population of these 30 counties totals 7,490,543, the approximate middle third of the total population of Texas, which is 21,779,893. Table 4.2 shows the target counties by population and their map location.

Table 4.2: List of Target Counties By Population

	Name	Population	Map Location
1.	El Paso	697,562	Far West
2.	Hidalgo	614,474	South
3.	Collin	566,798	North Central
4.	Denton	488,481	North Central
5.	Fort Bend	399,537	Upper Coast
6.	Cameron	353,561	South
7.	Montgomery	328,449	Upper Coast
8.	Nueces	314,696	Coastal Bend
9.	Williamson	289,924	Central
10.	Galveston	261,219	Upper Coast
11.	Brazoria	257,256	Upper Coast
12.	Jefferson	248,890	Upper Coast
13.	Lubbock	247,574	South Plains
14.	Bell	244,668	Central
15.	McLennan	217,713	Central
16.	Webb	207,611	South
17.	Smith	181,437	Northeast
18.	Brazos	156,099	Central
19.	Johnson	136,332	North Central
20.	Whichita	129,964	Rolling Plains
21.	Taylor	125,647	West Central
22.	Ector	122,312	Far West
23.	Ellis	120,052	Central
24.	Midland	117,669	Far West
25.	Potter	116,093	Plains
26.	Grayson	113,860	North
27.	Gregg	113,255	Northeast
28.	Hays	109,570	South West
29.	Randall	106,822	Panhandle
30.	Tom Green	103,018	West Central
		TOTAL	7,490,543

See Appendix D for location of target counties.

Statistics

In the case of this particular study, simple frequency distribution statistics is used. Frequency distribution shows the number of times that the various attributes of a variable are observed in a sample (Babbie, 2001, p. 398). This technique for presenting data is very useful in describing the strengths and weaknesses in the cyber security tools utilized by Medium-sized Texas Counties.

Once it is determined what type of data is to be gathered, that data must be organized. Once data is organized, it is easier to understand the implications of the findings produced by the data. The next chapter organizes and summarizes those findings, while the last chapter uses those findings to provide conclusions and implications for the results. See Appendix A for survey instrument example, Appendix B for Background Data profile, and Appendix C for subject area profile.

CHAPTER FIVE

RESULTS

The purpose of the results chapter is to organize and present the findings of the survey data. Results are organized using the conceptual framework presented in Chapter 4, and the survey instrument as presented in Appendix A. Major security tools consisted of needs assessment, security policy, security system components, system auditing, and incident response plan.

Background Data

The particular job titles of those who were in charge of information technology were very diverse. These titles are as follows: Director of Information Technology, Director of Information Services, Director of Communication and Information Services, Information Technology Manager, Director of Information Systems, and Director of Management Information Systems.

The number of information technology (IT) staff employed by the counties that responded to the survey range from 4 to 19, which calculates into an average of 10 IT staff per county.

Eight of the thirteen counties indicated that they contract out for some of their computer services. The most common types of services contracted out for were network services, hardware & software maintenance, application support and Internet access.

Twelve of the respondents stated that cyber terrorism was a concern in their county. When asked if their computer systems had experienced any security violations within the last year, nine of the thirteen respondents indicated that they had experienced security violations. Of the nine that had experienced security violations, all indicated that a virus infection was the cause of the security violation.

Table 5.1: Summary of Background Information

Background Information	**Frequency # Indicating Yes**
General Information	---
Personnel directly involved in computer operations	4-19 Avg. 10
Computer Related Information	---
Does County Contract out for any computer services?	8
Is Cyber Terrorism a concern?	12
Has the county received security breaches within the past year?	9
If yes, what types of violations have you experienced	*9 experienced viruses

* Eight of the nine counties that experienced virus infections, all used packet-filtering firewalls, stateful inspection firewalls, or both. The other county that experienced a virus used packet-filtering firewalls and application proxy firewalls. The four that did not receive any security violations within the year used application proxy firewalls only.

Computer Security Needs Assessment

Computer security needs assessment, as discussed in Chapter 3, consists of three stages. Those stages consist of the initial stage, development stage and the selection stage. The initial stage revealed that eight of the thirteen counties had conducted a computer security needs assessment. Of those eight, everyone had gone on to the development stage. The needs assessment was done prior to development of the security policy. The third stage of the needs assessment was the selection stage. Six of the eights respondents indicated that they conducted the needs assessment prior to the selection of the computer security system deployed by the county. Six of the counties have all of the components of a needs assessment in place.

Table 5.2: Summary of Computer Security Needs Assessment

Needs Assessment	Frequency # Indicating Yes
Initial Stage	---
Has county conducted a computer security needs assessment?	8
Development Stage	---
Was the needs assessment done prior to development of security policy?	8
Selection Stage	---
Did the needs assessment influence the essential functions of the selected or created security system?	6
Number that had all components of the needs assessment?	6

Computer Security Policy

Computer security policy can be divided into three stages. The initial stage identifies whether the county has a computer security policy in place, the update stage identifies if the counties that have policies in place update them on a regular basis, and the responsibility stage identifies if there are specific areas in the policies that discuss the roles and responsibilities of the organization and employees.

In the initial stage, almost all (12 of 13) counties have computer security policies in place. In the second stage, of those twelve that had policies in place nine stated that they updated their security policies on a regular basis in order to stay current with the county security needs. The third stage identifies whether or not the counties computer security policy includes responsibilities of both the organization and employees. Of the twelve counties that have computer security policies in place, all twelve have areas in their policy that include a discussion of security responsibilities, eleven have areas that include penalties for noncompliance in their policy, two include procedures for network intrusion in their policy, seven include procedures for computer backup in their policy and five include procedures for restoration and classification of information in their policy. Only two of the counties have all of the policy components in place.

Table 5.3: Summary of Computer Security Policy

Computer Security Policy	Frequency # Indicating Yes
Policy in Place	**---**
Are there written policies in place for computer security?	12
Policy Updated Regularly	---
Is the security policy updated on a regular basis to stay current with county security needs?	9
Include Responsibilities of Both the Organization and Employees	---
Does the security policy include a discussion of security responsibilities?	12
Does the security policy include penalties for noncompliance?	11
Does the security policy include procedures for network intrusion?	2
Does the security policy include procedures for backup?	7
Does the security policy include procedures for restoration and classification of information?	5
Number with all of the components of the policy?	2

Cyber Security Protection Components

The cyber security protection components consisted of five major deterrence mechanisms for protecting computer systems. Those protection components are intrusion detection systems, router security, firewall, anti-virus software, and password protection. In the area of intrusion detection system protection, nine of the thirteen counties indicated that they utilize intrusion detection system. All nine of the counties stated that the intrusion detection system provided twenty-four hour/seven days a week (24/7) protection. Seven of the nine counties that utilize intrusion detection system protection stated that it identifies, alerts and presents all anomalous activity. Seven of the nine counties also indicated that their intrusion detection system provides misuse detection. Seven of the nine counties stated that their intrusion detection systems also had router security protection included in them.

Twelve of the thirteen counties indicated that they use firewalls. Of those twelve that use firewalls all stated that their firewalls control traffic entering and exiting the system. In response to what type of firewall each county uses, three indicated that they use packet-filtering firewalls only. Four of the counties stated that they use packet-filtering and stateful inspection firewalls. Four of the counties indicated that the use application proxy firewalls only, and one stated that they use packet-filtering firewalls and application proxy firewalls.

The responding counties scored high in the area of anti-virus protection. All thirteen counties use anti-virus software, and eleven of those respondents indicated that their anti-virus software automatically updates its antidotes. Nine of the respondents stated that they run their anti-virus software daily, with the remaining four indicating that the anti-virus software was at minimum run weekly.

The responding counties also scored high in the area of password protection. All thirteen respondents stated that they use password protection. Of those thirteen respondents, only one indicated that they instruct employees to change their passwords every thirty days, four stated that they instruct employees to change their passwords every sixty days, four indicated that they instruct employees to change their passwords every ninety days, and four stated that they seldom instruct employees to change their passwords. Eleven of the thirteen counties indicated that they instruct county employees to use upper case letters, lower case letters, numbers, and signs in their passwords. Five of the thirteen counties had all of the cyber security protection components in place.

Table 5.4: Summary of Cyber Security Protection Components

Cyber Security Protection Components	Frequency # Indicating Yes
Intrusion Detection Systems Protection	---
Are intrusion detection systems utilized?	9
Does the intrusion detection system provide 24/7 protection?	9
Does the intrusion detection system identify, alert and present all anomalous activity?	7
Does the intrusion detection system provide misuse detection?	7
Router Security Protection	**---**
Does the intrusion detection system also have router security included in it?	7
Firewall Protection	---
Does the county use firewalls?	12
Do the firewalls control traffic entering and exiting a system?	12
Are packet-filtering firewalls used?	8
Are stateful inspection firewalls used?	4
Are application proxy firewalls used?	5
Anti-Virus Protection	---
Does your county use anti-virus software?	13
Does your anti-virus software automatically update its antidotes?	11
Is the anti-virus software run daily?	9
Is the anti-virus software run weekly?	4
Is the anti-virus software run monthly?	0
Is the anti-virus software run annually?	0
Is the anti-virus software never run?	0
Password Protection	---
Does the county use password protection?	13
Are passwords changed every thirty days?	1
Are passwords changed every sixty days?	4
Are passwords changed every ninety days?	4
Are passwords seldom changed?	4
Do you instruct users to use upper case letters, lower case letters, numbers, and signs in there passwords?	11
Number that had all of the components?	5

Computer System Auditing

The responding counties scored low in the area of computer system auditing. Only six of the thirteen respondents indicated that they have a system auditing process in place. All of the counties that have a system auditing process in place indicated that the audits are performed on regular schedule intervals. All six counties also stated that if revisions were indicated by the audit, they have a system in place to implement any changes necessary. Six of the counties had all of the computer system auditing components in place.

Table 5.5: Summary of Computer System Auditing

Computer System Auditing	Frequency # Indicating Yes
Auditing Process in Place	---
Is there a system auditing process in place?	6
Audits Done Regularly	---
If yes, Are the audits performed on regular schedule intervals?	6
System for Implementing Change	---
If revisions are indicated, do you have a system in place to implement change?	6
Number that had all of the auditing components in place?	6

Computer Incident Response Plan

In the area of incident response, nine of the thirteen respondents indicated that they have incident response plans in place. Of those nine with plans in place, only 5 have tested their system in a county drill or emergency situation. Seven of the nine counties with incident response plans in place, examine and modify its effectiveness against newly defined security threats. Five of the thirteen counties have all of the components of a computer incident response plan.

Table 5.6: Summary of Computer Incident Response Plan

Computer Incident Response Plan	Frequency # Indicating Yes
Incident Response Plan in Place	---
Is there a system computer incident response plan in place?	9
Plan Tested	---
If yes, has the system been tested in a county drill or emergency situation?	5
Plan Examined	---
Is the program examined and modified to ensure its effectiveness against newly defined security threats?	7
Number that had all components of the incident response plan	5

CHAPTER SIX

CONCLUSION

Research Summary

The purpose of this research study was three fold. First, the purpose was to develop a model framework for countering cyber terrorism. The scholarly literature was used as the springboard for the Cyber Security Model. The model organized defense tools that should be used to protect medium-sized Texas counties from a terrorist attack. The second purpose was to assess security systems of medium-sized Texas counties using the model framework. In order to address the second purpose, a survey was developed from the conceptual framework and sent to the 30 identified counties to determine what tools they had in place to counter a cyber terrorist attack. Finally, this study is intended to develop recommendations that will improve computer security systems used by medium-sized Texas counties to counter cyber terrorism.

Table 6.1 identifies the overall findings of medium-sized Texas counties cyber security systems. The small response rate makes generalization difficult. The table is listed in order of assignment as identified in Chapter 3. The results of the findings are identified by using 1) unanimous support, 2) strong support, 3) modest support, and 4) varied support. Unanimous support is when all 13 counties have the security component in place. Strong support is when at least 9 of the counties have the security component in place, but no more than 12. Modest Support is when at least 5 of the counties have the security component in place, but no more than 8. Varied Support is when the counties range from as many as 12 to as few as 5 within the same component.

The survey revealed an average overall outcome for the basic cyber security components. The majority of the responses in most areas were modest support. Needs Assessment, Intrusion Detection Systems Protection, Router Security Protection, System Auditing and Incident Response Plan all showed an overall rating of modest support. Anti-virus software protection, password protection and firewall protection all showed an overall rating of strong support. Security Policy showed an overall rating of strong support with regard to having a policy in place and the policy being updated regularly, but had varied support when it came to policy responsibilities.

The research revealed that all of the counties had some of the security components recommended for a cyber security system; however in the security policy component, the counties have not done an adequate job of including responsibilities. The research also shows that 12 of the 13 counties use firewalls, and that the only four counties that did not receive any security violations within the year used application firewalls only. All of the other counties (9) experienced security violations within the year. Only two (2) of the counties had all of the defense components identified in the model and they were two of the four counties that did not experience security violations.

Recommendation

This leads to the recommendation of each county re-assessing their cyber security needs and existing security systems. Developing a comprehensive cyber security system will:

- Reduce vulnerabilities to a cyber attack.
- Provide for a uniform approach to cyber security protection
- In the event of an attack provide an immediate response plan to minimize damage

Considering how much of our day-to-day functions in addition to our national defense system that is dependent on the computer system, it is crucial that all public and private sectors take every step necessary to ensure cyber security.

It is also very important that the counties do more than have policies in place. Those policies must apply against the different components and then fine-tune the policies with the latest technology. The problem is that many organizations are forcing policies better suited for the old mainframe model onto today's environments of notebooks and mobile computing. The ultimate goal should entail every cyber system component matching the policy.

There is no one solution to cyber security, yet by combining the tools of needs assessment, computer policy, computer system components, computer auditing and an incident response plan, the stage will be set for effectively countering a cyber terrorist attack. A well-planned security system can help ensure continuing productivity by reducing the likelihood of hacker attacks, viruses and internal security risks in networks. At the same time, it can help companies avoid the expenditures that become necessary when a breach in security occurs. These tools, if utilized, will become an important piece in any good cyber security model.

Going back to the football coach analogy identified in Chapter 3, if only a few of the players were fully prepared, the team's chances of winning the game would be unlikely. Medium-sized Texas counties face the same challenge. If the counties only have a couple of the security components in place, their chance of stopping a cyber terrorist attack would be minimal.

Suggestions for Further Research

This concludes this research project. A further study of the cyber security measures of medium-sized Texas counties should be made, especially in light of the 43 percent response rate in this present research. In the future, other studies could be made comparing the cyber security components used in medium-sized Texas counties to the cyber security components used in other Texas counties, both small and large, or even all three. Another angle of research could be to do a case study of a local, state or federal department and assess their cyber security components compared to those identified in the cyber security model.

One of the main contributions of this particular research is the questionnaire that was developed to gather the data for the counties. Do to its simplicity, counties, or other organizations, could use this questionnaire as a start for identifying components to help address the problem of cyber terrorism.

Table 6.1: Summary of Findings

Summary of Research Findings		
Model	Component	Overall
Needs Assessment	**********************	Modest Support
• Initial Stage	Modest Support	
• Development Stage	Modest Support	
• Selection Stage	Modest Support	
Security Policy	**********************	Strong Support
• Policy in place	Strong Support	of policy, but
• Policy updated regularly	Strong Support	Varied Support
• Policy includes responsibilities	Varied Support	of responsibilities
Computer Security System Protection Components		
• **Intrusion Detection Systems Protection**	**********************	Modest Support
1. System utilized	Strong Support	
2. Provide 24/7 protection	Strong Support	
3. Identify, alert & present	Modest Support	
4. Provide misuse detection	Modest Support	
• **Router Security Protection**	**********************	Modest Support
1. Included in Intrusion Detection	Modest Support	
• **Firewall Protection**	**********************	Strong Support
1. Use Firewalls	Strong Support	of use of
2. Firewalls control traffic	Strong Support	firewalls, but
3. Packet-filtering used	Varied Support	Varied Support
4. Stateful inspection used	Varied Support	on type used.
5. Application proxy used	Varied Support	
• **Anti-Virus Software Protection**	**********************	Strong Support
1. Use anti-virus software	Unanimous Support	
2. Automatically update	Strong Support	
• **Password Protection**	**********************	Strong Support
1.Use password protection	Unanimous Support	
2. Instruction to users	Strong Support	
System Auditing	**********************	Modest Support
• Auditing process in place	Modest Support	
• Audits done regularly	Modest Support	
• System for implementing change	Modest Support	
Incident Response Plan	**********************	Modest Support
• Incident plan in place	Modest Support	
• Plan tested	Modest Support	
• Plan examined	Modest Support	

May 16, 2003

Dear Information Technology (IT) Director/Manager:

My name is Gerard Bickham and I'm a Purchasing Manager with the City of Austin. I am also a graduate student in the MPA program at Southwest Texas State University and currently working on my applied research project to fulfill the requirements for my degree. I would like to request your participation in a short survey.

The intent of this survey is to examine the types of cyber security measures currently in place within medium-sized counties within the state of Texas with populations that range from 100,000 to 700,000. This research uses a cyber security model to assess the cyber security preparedness of medium-sized Texas counties. The survey will take no longer than 10 minutes.

Due to the sensitive nature of the material, your responses will be kept confidential and only group statistics will be reported. All information will be used for research only. Although participation is strictly voluntary, I encourage all directors/managers to participate so that enough data will be received to achieve statistical integrity. If there is someone in your department who is more appropriate to respond to this survey, please feel free to forward it to them for completion.

Thank you very much for your time and cooperation. If you have any comments or questions, please feel free to contact me. Your response is requested by May 30, 2003.

Thank you for participating in this survey.

Sincerely,

Gerard Bickham, CPM
Purchasing Manager
City of Austin, SWS
(512) 974-3594

APPENDIX A

SURVEY INSTRUMENT

Cyber Security System Program Survey Of Medium-Sized Texas Counties

Part 1: Introduction

The intent of this survey is to examine the types of cyber security measures currently in place within medium-sized counties within the state of Texas. Due to the sensitive nature of the material, all responses and information provided will be kept strictly confidential. Thank you very much for your time and cooperation.

Part 2: Background Information

A. What is your job title? ______________________________

B. How many personnel are directly involved in computer operations? (e.g. programmers, system analysts, etc.) _______________

C. Do you contract out for any of your computer services? (from other governments, vendors, etc)? ______

D. If you do contract out for services, which services do you contract for?

____

E. Is Cyber Terrorism a concern in your county?

F. Has your computer system experienced any security violations within the last year? (e.g. virus infection, identity theft, etc?) _____________

G. If yes, what types of violations have you experienced?

____

Note: Check Yes or No unless otherwise indicated for questions 1 through 32.

Security System Needs Assessment	Yes	No
1. Has your county conducted a computer security needs assessment?		
2. Was the needs assessment done prior to development of a security policy?		
3. Did the needs assessment influence the essential functions of the selected or created security system?		
Security Policy		
4. Are there written policies in place for computer security?		
5. Is the security policy updated on a regular basis to stay current with county security needs?		
6. Does the security policies include a discussion of security responsibilities?		
7. Does the security policy include penalties for noncompliance?		
8. Does the security policy include procedures for network intrusion?		
9. Does the security policy include procedures for backup?		
10. Does the security policy include procedures for restoration and classification of information?		
Cyber Security System Protection Components		
11. Are intrusion detection systems utilized?		
12. Does the intrusion detection system provide 24/7 Protection?		
13. Does the intrusion detection system identify, alert and present all anomalous activity?		
14. Does the intrusion detection system provide misuse detection?		
15. Does the intrusion detection system also have router security included in it?		
16. Does the county use firewalls?		
17. Do the firewalls control traffic entering and exiting a system?		
18. Are packet-filtering firewalls used?		
19. Are stateful inspection firewalls used?		
20. Are application proxy firewalls used?		
21. Does your county use anti-virus software?		
22. Does your anti-virus software automatically update its antidotes?		
23. Is the anti-virus software run daily _____, weekly ______, monthly ______, annually ______, or never _______? Please check those that apply.		
24. Does the county use password protection?		
25. Are passwords changed every thirty days ______, sixty days _____, ninety days _____, or are they seldom-changed _____?		
26. Do you instruct users to use upper case letters, lower case letters, numbers, and signs in there passwords?		

System Auditing		
27. Is there a system auditing process in place?		
28. If yes, are the audits performed on regular schedule intervals?		
29. If revisions are indicated, do you have a system in place to implement change?		
Incident Response Plan		
30. Is there a computer incident response plan?		
31. If yes, has the system been tested in a county drill or emergency situation?		
32. Is the program examined and modified to ensure its effectiveness against newly defined security threats?		
33. ADDITIONAL COMMENTS: If you have any additional comments regarding your organization's computer security, feel free to comment in this section.		

APPENDIX B

BACKGROUND DATA PROFILE

Part 2: Background Data

A. This information is used to determine the exact job title of the person in charge of the Information Technology (IT) Section, due to the lack of standardized IT titles within Texas counties.

B. This question is used simply to determine how many personnel are actually involved in computer operations.

C. This information is used to determine how many respondents contract for their computer services needs.

D. This information is used to determine what types of services the respondents contract for.

E. This information is used to determine if cyber terrorism is a concern of the county.

F. This information is used to determine whether or not respondents had experienced security violations.

G. This question is used to determine what types of security violations the county experienced.

APPENDIX C

SUBJECT AREA PROFILE

Note: All question in Subject Area Profile are used to determine if certain model cyber security tools are in place to guard against cyber terrorism.

Part 3: Security System Needs Assessment

Questions 1, 2, and 3 are used to determine whether or not respondents have performed the initial stage of the cyber security model, which is conducting a "needs assessment."

Part 4: Security Policy

Questions 4,5, and 6 are used to determine whether or not respondents have performed the next stage of the cyber security model, which is establishment of computer security policy and procedures and to determine whether the policies are updated on a regular basis to stay current with county security needs.

Part 5: Cyber Security System Components

Questions 7 through 26 are used to determine whether or not respondents have cyber security system components in place as described in the cyber security model.

Part 6: System Auditing

Questions 27, 28, and 29 are used to determine whether or not respondents have a system auditing process in place and determine whether this process is performed on regularly scheduled intervals.

Part 7: Incident Response Plan

Questions 30, 31, and 32 are used determine whether or not respondents have an incident response plan in place and if they do, determine whether or not the system has been tested.

Additional Comments

Question 33 is used to gather information and insights from respondents that cannot be gathered in the form of predetermined response categories.

APPENDIX D

MAP OF TEXAS COUNTIES

Bibliography

American National Standards Institute, Inc. (February 28, 2001). American National Standard for Telecommunications – Telcom Glossary 2000. *Prepared by T1A1 Technical Subcommittee on Performance and Signal Processing*. [On-line]

Andrews, Lyde. (August 28, 2001). Ok, So I Need Security. Where Do I Start. *Indiana University of Pennsylvania: Library Resources*. [On-line] http://www.lib.iup.edu/comscisec/SANSpapers/andrews.htm

Babbie, Earl. (2001). *The practice of social research, 9th ed.* Belmont, CA: Wadsworth Publishing Company.

Balzer, Bob. (9/24/02). *Two in Reserve: A Policy for Countering Cyber-Terrorism*. [On-line]: http://www.isi.edu/gost/cctws/balzer.html

Bennett, Robert F. (May 2002) Security in the Information Age: We're Not in Kansas Anymore. *Study done for the U.S. Joint Economic Committee entitled "Security in the Information Age: New Challenges, New Strategies."*

Blake, Scott. (n.d.). Computer Security: Protecting the Network Neighborhood. *Security Management Online*. Retrieved January 31, 2003, from http://www.securitymanagement.com/library/000833.html

Brindley, Adrian. (November 1, 2002). Denial of Service Attacks and the Emergence of "Intrusion Prevention Systems". *SysAdmin, Audit, Network, Security (SANS) Institute*. [On-line] http://www.sans.org/rr/firewall/prevention.php

Cheng, Lebin. (n.d.). Virtual Private Corporation: Information Security Infrastructure Restructuring Strategy for Countering Cyber-Terrorism. *Hewlett-Packard Company*. [On-line] http://www.isi.edu/gost/cctws/lebinc.html

Cisco Systems, Inc. (August 2, 2002). *Building In-Depth Security for Small and Midsize Business Networks,* 1-15

Clarke, Suzy. (November 2002). Case Study in Information Security. *SysAdmin, Audit, Network, Security (SANS) Institute, 1-19*

Clyde, Robert. (July 1, 2001). GOVERNMENT TECHNOLOGY/ Protecting computers from malicious code. *American City and County*. [On-line] www.americancityandcounty.com

Dedge, Pamela. (October 15, 2001). Fighting Cyber Terrorism-Where do I Sign Up? *SysAdmin, Audit, Network, Security (SANS) Institute*. [On-line] **http://www.sans.org/rr/firewall/fighting.php**

Denning, Dorthy E., (February 4, 2000). Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. *Nautilus Institute.* Pages 1-34

Denning, Dorothy E., (May 23, 2000). Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives. *Nautilus Institute.* Pages: 1-34

Department of Information Resources (DIR). (June 7, 2002) *IS Security Policies: Policy Guide*. Austin, Texas: DIR

Dunham, Griffin S. (2002). Carnivore, The FBI'S E-mail Surveillance System: Devouring Criminals, Not Privacy*. Indiana University School of Law. Pages 544-566*

Dunn, Scott. (September 2002). Windows Tips: Keep Prying Eyes at Bay With Windows' Passwords. *PC World Magazine*

Ellis, Chris. (February 2003). '7 Steps' for network security. *Communications News*, Vol. 20, Issue 2; pg. 36, 2 pgs

Farshchi, Jamil. (n.d.) Statistical based approach to Intrusion Detection. SysAdmin, Audit, Network, Security (SANS) Institute. Retrieved on January 31, 2003 from http://www.sans.org/resources/idfaq/statistic_ids.php

Fourie, Glenn. (May 8, 2002). The Evolution of the Information Security Mindset: A Hypothesis of Stages of Individual and Enterprise Security Maturation. *SysAdmin, Audit, Network, Security (SANS) Institute*. [On-line] http://www.sans.org/rr/modeling/mindset.php

Gidh, Ajay. (March 10, 2003). Why disaster recovery planning? *Express Compute*

Gips, Michael A. (n.d.). Computer Security: Is Your Web Site a Hacker's Delight? *Security Management Online*. Retrieved on January 31, 2003 from http://www.securitymanagemet.com/library/000713.html

Ginski, Richard. (June 22, 2001). Information Security Implementation for a Local Government. *SysAdmin, Audit, Network, Security (SANS) Institute*. [On-line]: http://www.sans.org/rr/casestudies/local_gov.php

Green, Meg. (February 2003). Securing The System. *Best's Review*

Haig, Leigh. (March 7, 2002). LaBrea - A New Approach to Securing Our Networks. *SysAdmin, Audit, Network, Security (SANS) Institute.* [On-line]: http://www.sans.org/rr/attack/labrea.php

Halme, Lawrence and Bauer, Kenneth. (n.d.) AINT Misbehaving: A Taxonomy of Anti-Intrusion Techniques. *SysAdmin, Audit, Network, Security (SANS) Institute*. Retrieved January 31, 2003, from http://www.sans.org/resources/idfaq/aint.php

Hogan, Beatrice. (October 2000). Turkmenistan, An Information Black Hole. *Business 2.0 Magazine*

Huffer, John. (February 18, 2002). Corporate Networks Need Multiple-Level Protection. *Business Journal*, 87506890, 2/18/02, Vol. 23, Issue 7

In both war and peace, computers face attack. (March 31, 2003). *Austin American-Statesman*, p. D1

Institute for Information Infrastructure Protection (I3P). (2003*). Cyber Security Research And Development Agenda.*

Institute for Security Technology Studies At Dartmouth College (ISTS). (September 22, 2001). *Cyber Attacks During The War On Terrorism: A Predictive Analysis*

Institute for Security Technology Studies At Dartmouth College (ISTS). (September 26, 2001). *Cyberterrorism: the State of U.S. Preparedness*. Before the House Committee on Government Reform Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations.

Internet Security Alliance. (n.d.). Frequently Asked Questions. *pcIntenet Control*. Retrieved on May 17, 2003 from http://www.pcinternetpatrol.com/faq/faq.php

Internet Security Systems (ISS). (September 28 – December 31, 2002). *Executive Summary: Internet Risk Impact Summary.*

Joint Economic Committee United States Congress, (May 2002). *Security In the Information Age: New Challenges, New Strategies*

Jones, Jennifer. (July 29, 2002) The promise of all-in-one security. *Network World.* Vol. 19, Iss.30: Pg. S12, 2 pgs.

Just, James. E. (n.d.). Some Useful Capabilities in Countering Cyber Terrorism. *Computer Crime Research Center*. [On-line] http:www.crime-research.org/eng/library/James2.htm.

Kent, S. and Atkinson, R. (November 1998). Security Architecture for the Internet Protocol. *The Internet Society 1-61.*

Kerschbaum, Florian, Spafford, Eugene, and Zamboni, Diego. (2002). Using internal sensors and embedded detectors for intrusion detection. *Journal of Computer Security10*, 23-70.

Lam, Wing. (May/June 2002). Ensuring Business Continuity. *IT Pro*, 19-25

Liston, Kevin. (n.d.) Can you explain traffic analysis and anomaly detection? . *SysAdmin, Audit, Network, Security (SANS) Institute*. Retrieved on January 31, 2003 from http://www.sans.org/resources/idfaq/anomaly_detection.php

McClure, David L. (July 11, 2001). Electronic Government: Challenges must be addressed with Effective Leadership and Management. *U.S. General Accounting Office (GAO)*

Middleton, Bruce. (n.d.). Computer Security: Mapping a Network Security Strategy. *Security Management Online*. Retrieved January 31, 2003, from http://www.securitymanagement.com/library/000619.html

Mitchell, Bradley. (August 8, 2002) Network Disaster Recovery. *Computer Networking*. [On-line] http://compnetworking.about.com/library/weekly/aa083102a.htm

National Institute of Standards and Technology (NIST), (December 2001) *Underlying Technical Models for Information Technology Security.* NIST Special Publication 800-33

Neeley, DeQuendre. (n.d.). Computer Security: You've Been Hacked…Now What*? Security Management Online*. Retrieved January 31, 2003, from http://www.securitymanagement.com/library/000797.html

O'Flaherty, Kristi. (November 12, 1999). Anti-virus Protection needed to keep Computers Healthy. *Fort Worth Business Press*

Overholt, Matt and Brenner, Professor. (Spring 2000). Overview of Cyber-Terrorism. *University of Dayton School of Law*. [On-Line] http://www.cybercrimes.net/Terrorism/overview.html

Robb, Drew. (April 2002). Protecting sensitive data requires vigilance. *HRMagazine*, Vol. 47, Issue 4: pg.91, 4 pgs.

Rodriguez (2001). Cyberterrorism- An Emerging Threat to National Security. *Inforware.Com* [On-line]: http://www.infowar.com/class_3/01/class3_112901a_j.shtml

Rogers (1999). Organized Computer Crime and More Sophisticated Security Controls: Which Came First the Chicken or the Egg? *Infoware.Com* [On-line]: http://www.infowar.com/survey/99/correlation1.shtml

Seltzer, Larry. (February 12, 2002). Solutions: Tools & Tips for the Internet Age: Password Crackers. *PC Magazine,* 68-71

Siegel, Carol A., Sagalow, Ty R., and Serritella, Paul. (September/October 2002). Cyber-Risk Management: Technical and Insurance Controls for Enterprise-Level Security. *Security Management Practices*, 33-49

Spencer, Ralph. (Spring 1997). Passwords: Obsolete Authenticators Or Cutting Edge*? Information Systems Security*, 1065898X, Spring97, Vol. 6, Issue 1

Sproles and Byars (1998). Examples of Cyber terrorism. [On-line]: http://www-cs.etsu-tn.edu/gotterbarn/stdntppr/cases.htm:

Sutherland, John. (April 11, 2001). 4th Generation of Linux Based Firewalls. *SysAdmin, Audit, Network, Security (SANS) Institute*. [On-line] http://www.sans.org/rr/firewall/4th_gen.php

Texas Association of Counties. (n.d.) The County Information Project: *Map of Texas Counties*. [On-line] http://www.county.org/cip/Products/CountyMap.pdf

The White House. (February 2003). *The National Strategy To Secure Cyberspace*. Retrieved March 31, 2003, from http://www.whitehouse.gov/pcipb/

Tirenen, Walter. (n.d.). White paper for a Strategic Cyber Defense concept: Deterrence Through Attacker Identification. *Computer Crime Research Center*. [On-line] http://www.crime-research.org/eng/library/White

Toulin, Alan. (January 15, 1999). Canada: New Technology a Bonanza for Crime-'Cyber-Terrorism' –FBI Director Calls Canada a 'Hacker Haven'. *Canada Financial Post*

U.S. Department of Commerce. (July 31,2002). *2001 Computer Security Survey*

Vatis, Michael A. (February 29, 2000). CYBERCRIME and the role of the National Infrastructure Protection Center. *Cybercrime Before the Senate Judiciary Committee, Criminal Justice Oversight Subcommittee and House Judiciary Committee, Crime Subcommittee*

Vimercati, S., Lincoln, P., Ricciulli, L. and Samarati, P. (2002). Global infrastructure protection system. *Journal of Computer Security 9*, 251-283

Vinciguerra, Paul. (November 17, 2001). A Layer-7 Secure Security Posture. *SysAdmin, Audit, Network, Security (SANS) Institute*. [On-line] http://www.sans.org/rr/firewall/layer7.php

Webb, Warren. (July 5, 2001). Guard Your Embedded Secrets. *EDN Magazine,* 52-58

West-Brown, Moira. (March 1999). Avoiding the Trial-by-Fire Approach to Security Incidents. *Security Matters*. Volume 2. Issue 1.