TABLE OF CONTENTS

ABSTRACT

Since September 11, 2001 terrorism was the chief concern among US citizens. Government officials were concerned on how to protect their communities from terrorism and immediately created and implemented various strategies and policies. Security experts and government officials felt that a cohesive partnership between businesses, government officials, scholars, universities, and private citizens would foster lines of communication in combating terrorism. With the creation of U.S. Department of Homeland Security, various publications outlined strategies to protect critical infrastructures and key assets. These strategies foster the partnership between government officials, businesses, and private entities and provided ideas for proactive measures in securing critical infrastructures. These strategies provided an avenue for this study.

The purpose of this study is threefold: (1) Identify and describe the potential cyber vulnerabilities and physical threats of water and energy infrastructures that are specified within documents outlined by the Department of Homeland Security (2) Identify and describe proactive measures in disaster recovery and information sharing that are specified within the literature review and documents outlined by the Department of Homeland Security and (3) Assess the Texas water and energy infrastructure vulnerability from the point of view of Texas Regional Council leaders.

This research assessed the Texas water & energy infrastructures vulnerability from the view point of Texas Regional Council leaders. The key areas of concern are physical security threats and vulnerabilities to computer systems. In addition, opinions

regarding disaster recovery and information sharing were reviewed. A survey instrument collected data and information from twenty – four Texas Regional Council leaders. Simple statistical methods were used to interpret the results.

The findings in the research demonstrated a high level of concern regarding vulnerabilities to cyber threats on both water and electricity infrastructures. In addition, respondents expressed a high level of concern with physical threats in both water and electricity infrastructures. The one caveat was the fire damage with relation to water systems. This particular threat was moderately received.

The majority of the respondents were moderately satisfied with the various disaster recovery planning methods in Texas local governments. Respondents expressed a moderate satisfaction with disaster recovery methods in both water and energy infrastructures in Texas local governments. Respondents were equally neutral and dissatisfied with the disaster recovery planning within Texas local governments. In addition, respondents expressed dissatisfaction with information sharing among government officials (local, state and federal) in both water and electricity infrastructures. They also expressed dissatisfaction with the information sharing regarding security measures and disaster recovery planning between local governments and private entities.

This study illustrates the concerns of these respondents who represent part of the Texas Homeland Security initiatives. These concerns echo the anxiety that most feel around the country. Security means safety. Citizens want accountability and would like to feel safe from terrorist acts. At this time, most terrorists are developing ways to exploit information and plan out innovative and disastrous attacks. Americans want to

feel safe in their communities. They look upon their government officials to provide this security for them.

CHAPTER ONE

Introduction

On September 11, 2001, the World Trade Centers in New York City were attacked and destroyed. The devastation in the wake of this catastrophe provided a chilling effect on the United States' economy and the world. Terrorists finally came and left a calling card. Since the attack, this burning image left other cities wondering if they will be the next target.

Protecting the critical infrastructure was the sounding call for all cities. Critical infrastructures are "systems and assets… so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, and any combination of those matters" (USA Patriot Act; The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, 2003, page 6). This issue became a critical concern for most cities and states across the country.

At the 70th Annual U.S. Conference of Mayors (USCM) Winter Meeting in January 2002, this concern was evident. Surveys were sent to 600 mayors in the U.S. through the collaboration of the USCM, Dupont and Cities United for Science Progress (CUSP) and 122 cities responded (CUSP, 2002, p.1). The survey focused on which threats were most concerning to mayors and the level of a city's emergency preparedness to deal with those threats (CUSP, 2002, p.1). It was apparent that mayors across the country were concerned with terrorist attacks. The results indicated that "concerns around chemical, biological and bomb threats are especially high" (CUSP, 2002, p.3). Considering that this survey was conducted eight months after 9/11, these mayors felt

these concerns needed to be addressed. The result indicated that "there is unexpected low satisfaction with preparedness to communicate with residents, businesses, and other jurisdictions and especially with healthcare providers" (CUSP, 2002, p. 4). Communication within the community needs to be addressed. Sharing information among government officials, businesses and residents is pertinent. Vast information concerning the safeguarding of lives and structures can be shared among government officials, businesses and residents. By sharing information, partnerships are formulated. Planning, coordinating tasks, and testing can navigate a fortified security plan. Sharing information is a proactive measure that is part of this applied research project. Along with information sharing, disaster recovery and/or a business contingency plans provide a safety net in the wake of a terrorist attack or disaster.

The CUSP survey also addressed threat detection. Mayors felt that there was a large shortfall in funding in association with threat detection and overwhelmingly, did not feel that their cities had enough personal protective apparel to meet the needs of their community in the event of a disaster or terrorist attack (CUSP, 2002, p. 6 and 8). Threat detection can be addressed in vulnerability assessment. Identification of critical infrastructures and key assets is the first step in assessing vulnerability. This applied research project addresses this issue in a platform outlined by the Department of Homeland Security.

The CUSP survey results were alarming and pose the question: How does Texas fair in preparedness and safeguarding the community from terrorist acts? Are critical infrastructures being protected from the potential threats that could be devastating to a

community in Texas? Like New York, how does Texas prevent this type of devastation from happening again?

This applied research project addresses some of these concerns that the CUSP survey discussed. In this applied research project, twenty-four respondents from the Texas Regional Councils of Government were surveyed on issues concerning physical threats and cyber vulnerabilities that may plague their water and electricity infrastructures. They were also provided questions regarding their perception of disaster recovery methods and information sharing among government officials and private entities. The respondents' answers could provide some knowledge of concerns on the vulnerabilities of water and electricity infrastructures in Texas. They could also offer some insight on how they felt on disaster recovery and information sharing in Texas.

Statement of the Research Problem

The purpose of this research is threefold: (1) Identify and describe the potential cyber vulnerabilities and physical threats of water and energy infrastructures that are specified within documents outlined by the Department of Homeland Security (2) Identify and describe proactive measures in disaster recovery and information sharing that are specified within the literature review and documents outlined by the Department of Homeland Security and (3) Assess the Texas water and energy infrastructure vulnerability from the point of view of Texas Regional Council leaders.

As a result of September 11, 2001, the Department of Homeland Security has made its mission to minimize terrorist acts against the United States and its interests. The Department of Homeland Security identified critical infrastructures as potential targets for terrorist acts. In this study, twenty-four respondents of the Texas Regional Councils

of Governments express their opinions and perception's relating to the security of two critical infrastructures: water and energy, as they relate to computer systems and physical security threats. The study explores these perceptions in order to apply a practical assessment of security measures that these regions can utilize.

Chapter Summaries

This applied research consists of six chapters. Chapter One provides an introduction to this research. Chapter Two provides an overview of various studies including insight on Texas Regional Councils of Government. Chapter Three describes the various components of the vulnerabilities that plague water and electricity infrastructures, and introduces the conceptual framework. Chapter Four describes the survey used to obtain data for this research project and introduces the operationalization of the conceptual framework. Chapter Five describes the perceptions of the Texas Councils of Government leaders about vulnerabilities to water and electricity systems in Texas, and summarizes the findings. Chapter Six provides an overall conclusion for this applied research project and also provides insight on future research on this subject matter.

CHAPTER TWO
SETTING

The purpose of this research is to assess the Texas water & energy infrastructures vulnerability from the view point of Texas Regional Council leaders. The key areas of concern are physical security threats and vulnerabilities to computer systems. In addition, opinions regarding disaster recovery and information sharing are reviewed. Each of these components is reviewed in depth in the following chapters. These elements formulate a conceptual framework that provides a roadmap in constructing a survey to obtain data for the assessment. The purpose of this chapter is to provide some background on why this subject matter became the focal point of this applied research project. Later in this section, Texas Homeland Security is discussed.

Following the September 11th attacks, strategies and reports were developed to combat terrorism. Using the reports listed below, the United States General Accounting Office (GAO) evaluated the state of security in the United States. (GAO report GA-04-408T):

- National Security Strategy of The United States of America;
- National Strategy for Homeland Security
- National Strategy for Combating Terrorism
- National Strategy to Combat Weapons of Mass Destruction
- National Strategy for the Physical Protection of Critical Infrastructure and Key Assets.
- National Strategy to Secure Cyberspace
- 2002 National Money Laundering Strategy

The GAO found that "none of the strategies addresses all of the elements for sources, investments, and risk management; or integration and implementation." GAO felt that *The National Strategy for Homeland Security* and *The National Strategy for the*

Physical Protection of Critical Infrastructures and Key Assets (Strategy) address the greatest number of desirable characteristics" (GAO -04-408T Highlights, February 2004). The *Strategy* was the most frequently cited document in this applied research project.

A "grand strategy" is necessary to provide the protection of our critical infrastructures. In a Joint Economic Committee, the United States Congress issued a report, "Security in the Information Age: New Challenges, New Strategies" on May 2002. "Because our vulnerabilities are complex and the threats are varied and unpredictable, it is impossible to protect everything from every threat."(Bennett, 2002, p. 3). Senator Bennett used this report to devise a "grand strategy" that would:

- Identify what is critical and vulnerable.
- Increase two-way information sharing between the public and private sectors.
- Improve analysis and warning capabilities."

Senator Bennett was not alone in devising and identifying the critical infrastructures, assessing vulnerabilities and sharing information between government and private sectors. The *Strategy* also called on these same strategies throughout its literature. Senator Bennett used Presidential Decision Directive 63 (PPD 63) on Critical Infrastructure Protection. "PPD 63 called for an initial vulnerability assessment within 180 days of issuance, followed by periodic updates for each sector of the economy and each sector of the government that might be a target of infrastructure attack" (Bennett, 2002, p. 3). In March 2001, the President's Council on Integrity and Efficiency issued a report with the following findings:

- "Most agencies had not identified their mission-essential infrastructure assets.
- Almost none of the agencies had completed their vulnerability assessments of their MEI (Mission Essential Infrastructure) assets or developed remediation plans." (Bennett, 2002, p. 3)

In September 2001, the GAO agreed with the findings. The GAO indicated that "while efforts to establish partnerships and raise awareness have been progressing, substantive, comprehensive analysis has not" (Bennett, 2002, page 4). Table 2.1 outlines the state of assessment and planning found by the committee:

TABLE 2.1 – Chart – Assessment in various sectors.

Infrastructure Sector	Vulnerability Assessment	Remedial Plan
Banking and finance	Some assessments	No remedial plan
Electric power, oil and gas	Some assessments	No remedial plan
Emergency fire services	No assessments	No remedial plans
Emergency law enforcement	No assessments	No remedial plans
Information and communications	No assessments	No remedial plans
Public health services	No assessments	No remedial plans
Transportation	No assessments	No remedial plans
Water supply	No assessments	No remedial plans

Source: Senator Robert F. Bennett, Joint Economic Committee, May 2002, p.4

Both of these reports indicated that some federal government agencies were not ready for terrorist attacks. This assessment became the focal point of this applied research project. The burning question: Where does Texas fare compared to its federal counterpart?

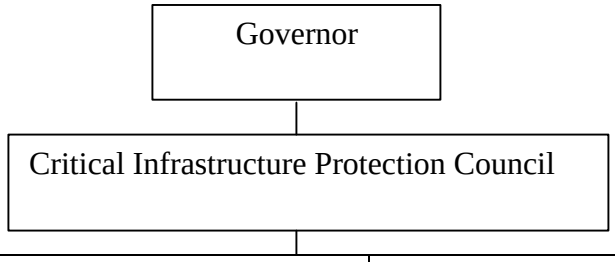
TEXAS HOMELAND SECURITY

Two weeks after September 11, 2001, Governor Rick Perry established a Task Force on Homeland Security to assess the state's response to potential terrorist attack. Former Texas Attorney General John Cornyn created the State Infrastructure Protection

Advisory Committee (SIPAC) to "work with local, state and federal government officials as well as private-sector experts to develop a strategy to protect state infrastructure and minimize disruption to critical services if these infrastructures are compromised" (Texas Homeland Security Strategic Plan, 2004, p. 6). This provided a foundation that has since evolved in the development of the *Texas Homeland Security Strategic Plan*. "Like its federal counterpart, this strategic plan encourages partnerships among local, state, and federal agencies, private sectors and volunteer groups" (Texas Homeland Security Strategic Plan, 2004, p. iii). The Texas Homeland Security office resides within the Governor's Office. On June 22, 2003, Governor Perry signed House Bill 9 that effectively created the Critical Infrastructure Protection Council (CIPC) (Texas Homeland Security Strategic Plan, 2004, p. 5). CICP serves as a focal command center to "coordinate the state's intelligence, warning and response system" (Texas Homeland Security Strategic Plan, 2004, p. 5).

The CICP is a group of state agencies that serve as a liaison between local governments and the governor's office, as well as between local governments and the private sector. These state agencies represent various sectors of the state infrastructure as illustrated in Table 2.2:

TABLE 2.2
Organizational Chart: Protecting Critical Infrastructures



Sector	**Lead Agency**
Air Quality	Texas Commission on Environmental Quality
Agriculture	Department of Agriculture
Criminal Intelligence	Department of Public Safety
Electricity	Public Utility Commission of Texas
Emergency Services	Governor's Division of Emergency Management – Texas First Responder Preparedness : **Texas Regional of Councils of Government**
Food Safety	Texas Department of Health
Government	Governor's Office
Information Services	Department of Information Resources
Military	Texas National Guard
Oil and Gas	Railroad Commission of Texas
Public Health	Texas Department of Health
Public Safety	Texas Department of Public Safety
Telecommunications	Public Utility Commission
Transportation	Texas Department of Transportation
Water	Texas Commission on Environmental Quality

Source: Texas Homeland Security Strategic Plan

The Critical Infrastructure Protection Council is required to have the following representatives per House Bill 9 (Texas Homeland Security Strategic Plan, 2004, p. 13):

- Governor's Office
- Department of Agriculture
- Office of the Attorney General
- General Land Office
- Public Utilities Commission
- Texas Department of Health
- Department of Information Resources
- Department of Public Safety
- Governor's Division of Emergency Management
- Texas National Guard
- Texas Commission on Environmental Quality
- Railroad Commission
- Texas Strategic Military Planning Commission
- Texas Department of Transportation

These agencies are part of the coordination of emergency response in case of a disaster or terrorist threat. One of Texas Homeland Security Program's Critical Mission Areas is the Emergency Preparedness and Response Team. Within the Emergency Preparedness and Response Team is the Texas First Responder Preparedness Program. The Texas Regional of Councils of Government (COG) is the "Regional Response Network" for the state (Texas Homeland Security Strategic Plan, 2004, page 19). The COGs are considered the "central component of the Regional Response Network in the Texas First Responders Preparedness Program." They are the nexus to every region and square mile within this state. COGs are vital because they interact with local, state, and federal agencies as well as private sector of the communities (Texas Homeland Security Strategic Plan, 2004, p. 19). The Texas First Responders consist of the following offices:

- Governor and Office of the Governor
- Division of Emergency Management
- Regional Councils of Government
- Office for Domestic Preparedness
- Texas Engineering Extension Services

Texas Regional Councils of Governments are vital to the Texas Homeland Security program. For this reason, Texas Regional Councils of Government is significant to this applied research project.

TEXAS REGIONAL COUNCILS OF GOVERNMENT

Texas Regional Councils of Government was created under the Regional Planning Act of 1965, Chapter 391, Local Government Code (Texas Association of Regional Councils (TARC), 2004). There are twenty-four Regional Councils of Government in Texas and coincide with the state's planning regions which are designated and reviewed by the governor (TARC, 2004). Under this law, COGs consists of "counties and municipalities making the agreement may join in the exercise of, or in acting cooperatively in regard to planning, powers, and duties as provided by law for any or all of the counties and municipalities" (TARC, 2004). The governing board for regional councils includes two-thirds local elected officials of cities and counties. "This quota allows the regional councils flexibility as to the composition of their boards, and some councils include citizen members or representatives of other groups on their governing bodies" (TARC, 2004). The governing board employs the executive director who oversees the daily operations of the COGs. Positions within regional councils may include: "director of regional planning, fiscal officer, regional service coordinator, planners, coordinators for aging, criminal justice, employment and training, environmental and other programs" (TARC, 2004). Bylaws and article of agreements

address the needs of the region and are not binding on member governments (TARC, 2004).

The Texas Association of Regional Councils (TARC) is a statewide association for these COGS. TARC's mission for COGs is to: "assist COGs in serving their local governments, provide a forum for exchange of information and ideas, educate other governmental agencies, citizens, and other organizations about COGs and their services and represent COGS at the state and national level" (TARC, 2004). COGs' responsibilities consist of providing assistance to local governments in: regional planning, reviewing applications for federal assistance, establishing and coordinating emergency communication, housing and economic development, environmental quality transportation and rural development (TARC, 2004). COG's role expands to include emergency response planning and homeland security initiatives.

"The Critical Infrastructure Protection Council coordinates with the twenty-four regional councils of governments and other local officials to ensure that every area of the state enhances emergency planning. Because terrorists seek to exploit a system's weakness, it is critical that each region have access to technical assistance and resources to safeguard its people and infrastructure" (Texas Homeland Security Strategic Plan, 2004, p.17). These COGs provide a significant role for the Regional Response Network.

The Texas Homeland Security Strategic Plan depicts COGs as a central component to its homeland security plan. "The state's 24 COG regions set the framework for the development of regional, interlocking and mutually supporting terrorism prevention efforts and preparedness programs. The use of regionally based and interlocking response systems promotes comprehensive planning and the collaborative

positioning of equipment and personnel. Each of these regions is approximately 200 miles in diameter, and they are based on the COG boundaries" (Texas Homeland Security Strategic Plan, 2004, p. 19). Since COGs are part of the Texas First Responder Preparedness Program, they are essential to the strategic plan.

Because COGs are the nexus to the Texas Homeland Security Program, they were the focus of this applied research project. In this applied research project, respondents from the Texas Regional Councils provide insight on their concerns regarding the various vulnerabilities that can disrupt and/or devastate an infrastructure. In addition, their views provide some insight on how they feel regarding disaster recovery methods and information sharing in Texas.

CHAPTER THREE
LITERATURE REVIEW

The purpose of this chapter is to review the literature relevant to the identification of potential vulnerabilities of water and energy critical infrastructures that are specified within documents outlined by the Department of Homeland Security. As the result of September 11, 2001, the Department of Homeland Security has made it their mission to minimize terrorist acts against the United States and its interests. Vulnerability assessments are the initial step in establishing security measures for our nation's critical infrastructure. This paper focuses on two vulnerabilities, computer systems and physical security threats. These key areas of concern are considered targets within public infrastructures. Terrorist groups target infrastructures because they can potentially cause the most devastating damage to cities and regions. In addition, this paper highlights proactive measures including information sharing and disaster recoveries to minimize these two types of vulnerabilities. In this section, various security measures are examined to address cyber and physical security vulnerabilities. The literature highlights various security models that address these threats. Identification of these threats provides a roadmap to establishing security measures.

Background – The Department of Homeland Security

The Department of Homeland Security (DHS) coordinates national efforts to secure America's critical infrastructure. Protecting America's critical infrastructure is the shared responsibility of federal, state, and local governments which are in partnership with the private sector. The private sector owns approximately 85 percent of our nation's critical infrastructure. The Department of Homeland Security embraces this partnership since it is responsible for coordinating a comprehensive national plan for protecting America's infrastructure. The Department gives state, local, and private entities one primary contact instead of many for coordinating protection activities with the federal government, including vulnerability assessments, strategic planning efforts, and exercises (*The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, 2003, p. 17). The Department of Homeland Security has identified sixteen critical infrastructure sectors essential to daily operations. They include:

CRITICAL INFRASTRUCTURES

- Agriculture and Food
- Banking and Finance
- Water
- Chemical Industry and Hazardous Materials
- Public Health
- Postal and Shipping
- Emergency Services
- National Monuments and Icons
- Defense Industrial Base
- Nuclear Power Plants
- Telecommunications
- Dams
- Energy
- Government Facilities
- Transportation

- Commercial Assets

Critical infrastructures are defined as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" (USA Patriot Act -National Strategy for Physical Protection of Critical Infrastructures and Key Assets, 2003). These sectors represent the core of America's society and have become the target of terrorist threats. Securing these infrastructures has become a priority since September 11, 2001.

The Department of Homeland Security is a result of the September 11, 2001 terrorist attacks and is the newest White House Cabinet office. On February 2003, The Department of Homeland Security along with the President's Critical Infrastructure Board released two strategies and documents that outline securing infrastructures: *The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets* and *The National Strategy to Secure CyberSpace*. These documents outline methods and strategies for fortifying public infrastructures. The essential component within these strategies have been the partnership of the federal, state, and local governments with the private sectors of the community that own and operate these infrastructures. Information sharing between the government and the public is the cornerstone in disseminating information should a disaster or terrorist attack occur. These strategies provide guidelines and instruction on how to handle the situation.

Table 3.1 highlights the various Presidential Decision Directives and Executive Orders that helped establish the Department of Homeland Security.

TABLE 3.1 – Presidential Decision Directives and Executive Orders

Title	Year	Agency Responsible	Description
Presidential Decision Directive 39 (PPD 39)	1995	Federal Bureau of Investigation	Develops the U.S. Policy on Counterterrorism. Federal Lead Agency for threats or acts of terrorism within the United States.
PPD 39	1995	Federal Emergency Management Agency	Directs FEMA with the support of all agencies in the Federal Response Plan.
Presidential Decision Directive 63 (PPD 63) [1]	1998	Department of Commerce	Creates Critical Infrastructure Assurance Office
PPD 63	1998	Federal Bureau of Investigations	Creates National Infrastructure Protection Center
PPD 63	1998	Information Sharing and Analysis Center	Develops a Partnership between Federal Lead Agencies and Private Infrastructure Sectors
PPD 63	1998	All Federal Agencies	Requires each federal agency to appoint a Chief Infrastructure Assurance Officer (CIAO)[2]
PPD 63	1998	President of the United States	Creates the National Infrastructure Assurance Council.[3]
Executive Order 13228	October 8, 2001	President of the United States	Creates the Department of Homeland Security
Executive Order 13321	October 16, 2001	President of the United States	Creates *The National Strategy to Secure Cyberspace*, February 2003[4]

[1] White Paper – the Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63., May 22, 1998

[2] White Paper – the Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63., May 22, 1998

[3] President will appoint a panel of major infrastructure providers and state and local government officials to serve on this council. President is the Chairman. White Paper – the Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63., May 22, 1998

[4] The Critical Infrastructure Protection Board coordinated efforts with local, state, and federal governments, private entities, and the American public to formulate "The National Strategy to Secure Cyberspace, February 2003

Various security-related agencies were consolidated to create the Department of Homeland Security. These agencies fall under four major division/directorates: The Border and Transportation Security; The Emergency Preparedness and Response; The Science and Technology; and The Information Analysis and Infrastructure Protection. Table 3.2 illustrates the various agencies that are part of U.S. Department of Homeland Security:

TABLE 3.2: U.S. Department of Homeland Security

Border and Transportation Security	**Emergency Preparedness**	**Science & Technology**	**Information Analysis and Infrastructure Protection: CIA, FBI, DIA and NSA**
U.S. Customs Service (Treasury)	The Federal Emergency Management Agency (FEMA)	CBRN Countermeasures Programs (Energy)	Critical Infrastructure Assurance Office (Commerce)
Immigration and Naturalization Service (Justice)	Strategic National Stockpile and the National Disaster Medical System (HHS)	Environmental Measurements Laboratory (Energy)	Federal Computer Incident Response Center (GSA)
The Federal Protective Services	Nuclear Incident Response Team (Energy)	National BW Defense Analysis Center (Defense)	National Communications System (Defense)
The Transportation Security Administration (Transportation)	Domestic Emergency Support Teams (Justice)	Plum Island Animal Disease Center (Agriculture)	National Infrastructure Protection Center (FBI)
Federal Law Enforcement Training Center (Treasury)	National Domestic Preparedness Office (FBI)		Energy Security and Assurance Program (Energy)
Animal and Plant Health Inspection Service (part) Agriculture)			
Office for Domestic Preparedness (Justice)			

Source: U.S. Department of Homeland Security website, 2004

The critical mission and strategies for Homeland Security are:

- "Identifying and assuring the protection of those infrastructures and assets that we deem most critical in terms of national-level public health and safety, governance, economic and national security and public confidence consequences;
- Assure the protection of infrastructures and assets that face a specific, imminent threat;

- Pursue collaborative measures and initiatives to assure the protection of other potential targets that may become attractive over time" (Strategy, p. 2-3, 2003).

Collaborating government entities and private sectors can improve the protection of public infrastructures and assets over time. Identifying these public infrastructures and ranking each based on importance takes time. A working relationship among government agencies and private entities can help establish these goals. Security strategies and methods can be discussed to entertain the various pros and cons for each.

The General Accounting Office recommends that agencies "take steps to complete the identification and analysis of their critical assets, including setting milestones and developing plans to address vulnerabilities" (GAO 03-233, Highlights, 2003). Identification of public infrastructures is paramount in addressing the vulnerabilities. The next section addresses various vulnerabilities pertinent to water infrastructures.

Water Infrastructures

Arnaud de Borchgrave, project director of the Center for Strategic and International Studies Task Force on Cyber Terrorism and Cyber Crime, indicates terrorists are gathering intelligence about our water resources. He suggests that some groups, possibly state operated terrorists, are downloading everything regarding the "water systems in the United States – reservoirs, canals, rivers, dams even the codes for opening and closing valves on the Hoover Dam" (Harris, 2000, p. 36).

Securing water resources is a daunting task. Water is a complex source where security of every river, canals, and reservoirs can be overwhelming. Computer systems

regulate and control some of these water systems. According to Professor Eric Byres, British Columbia Institute of Technology and an expert in critical information protection, "Some of the systems are so old even the hackers can't talk to them" (Chiruvolu, 2003). Old water systems may be found in rural areas of the country. Antiquated systems are difficult to secure.

Although no known terrorist attack on infrastructures has been reported, information on U.S. computerized water systems was discovered on computers found in al Qaeda camps in Afghanistan according to Richard Clarke, former special adviser to the president for cyberspace security (Hulme, 2003).

According to the *Strategy* report, the water sector consists of two basic components: fresh water supply and wastewater collection and treatment. There are 170,000 public water systems in the United States. They consist of reservoirs, dams, wells, aquifers, treatment facilities, pumping stations, aqueducts and transmission pipelines (Strategy, 2003, p. 39). In Texas, there are approximately 6,672 public water systems serving 20.04 million people (Texas Natural Resource Conservation Commission, 2001 Annual Report, p. 2).

The *Strategy* report features each infrastructure and provides challenges and initiatives for each infrastructure. The Water Sector challenge includes:

- Physical damage or destruction of critical assets, including intentional release of toxic chemicals;
- Actual or threatened contamination of the water supply;
- Cyber attack on information management systems or other electronic systems; and

- Interruption of services from other infrastructure.

The report recommends that the water sector increase monitoring and the capability to detect foreign substances in the water including biological, chemical or radiological contaminates (*Strategy*, 2003, p. 40). Initiatives for the Water Infrastructure include:

- Identify high-priority vulnerabilities and improve site security;
- Improve sector monitoring and analytic capabilities;
- Improve sector-wide information exchange and coordinate contingency planning;
- Work with other sectors to manage unique risk resulting from interdependencies.

Energy Infrastructure

Energy is another critical infrastructure that will be examined for this applied research project. Electricity, oil and natural gas are classified under this infrastructure. There are 2,800 power plants and 300,000 producing sites for oil and natural gas according to the *Strategy* report (*Strategy*, 2003, page 9). Unlike the other 48 states who share power grids that cross state lines, Texas has its own electric power grid.[5]

In Texas, the Electric Reliability Council of Texas, Inc (ERCOT) is the corporation that administers the state's power grid. ERCOT is one of 10 regional reliability councils in North America (ERCOT, 2004). According to the Texas Public Utility Commission, there are 85 power generation companies, 113 power marketers and 68 retail electric providers registered and/or certified in Texas (Texas Public Utility Commission, 2003, p. 58).

[5] This proved advantageous during the cascading power outage that occurred in the Northeast on August 14, 2003. Since Texas does not share an electrical grid with other states, Texas was not affected by the blackouts that seized the Northeast and Canada.

This applied research project examines the electricity sector and fresh water sector infrastructures. Focusing on these two segments of the infrastructure allows the researcher to survey respondents. Fresh water and electricity resources are generated across Texas, whereas oil refineries and gas are concentrated in certain areas of the state. The key concept is to identify these fresh water resources and electricity sectors.

The *Strategy* report's first objective is "to identify and assure the protection of those asset, systems, and functions that we deem most 'critical' in terms of national-level public health and safety, governance, economic and national security, and public confidence" (Strategy, 2003, p. 2). Identifying and protecting critical infrastructures is the initial step. Assessing these systems' vulnerabilities is the next step. "Threats to critical infrastructure fall into two general categories: (1) physical attacks against the "real property" components of the infrastructures, and (2) cyberattacks against the information or communications components that control these infrastructures" (Juster and Tritak, 2002, p. 12). Identification of these threats provides a roadmap to establishing security measures.

COMPUTER SYSTEM/CYBER VULNERABILITIES

Critical infrastructures are interconnected with computer systems. Computers control water systems and electricity sectors to operate and regulate their consumption. Daily activities rely on computer systems. Banks, businesses and government depend on computers to conduct business. Cyber terrorism is a security concern for our infrastructure. This interconnectivity comes with a high price. The interconnection of our physical assets and cyber assets make them vulnerable to computer based attacks (GAO 03-233, February 2003).

CYBERTERRORISM

In May 23, 2000, Dorothy E. Denning of Georgetown University testified before the Special Oversight Panel on Terrorism Committee on Armed Services and the U.S. House of Representatives. Ms. Denning provides the Committee compelling facts about cyberterrorism. Ms. Denning defines cyberterrorism as "the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attacks against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives" (Denning, 2000). Citizens of this country rely on computer systems to provide basic services to meet their needs. When services are disrupted, the public incessantly becomes concerned with costs and damages inflicted on the infrastructure. These attacks can cost millions of dollar to fix and prevent future attacks. In her testimony, Ms. Denning states that the ILOVEYOU Virus was estimated to hit millions of users and cost billions of dollars in damage. Preventative measures could have limited these vulnerabilities. Companies address these vulnerabilities after their systems have been compromised. Costs are either written off or not reported. Companies pass the cost on to consumers by way of higher fees or prices.

In her testimony to the U.S. House, Ms. Denning cites several published studies where critical infrastructures are "potentially vulnerable to cyberterrorist attack." In 1997, the Department of Defense conducted an exercise and found "the power grid and emergency 911 systems had weaknesses that would be exploited by an adversary using only publicly available tools on the Internet" (Denning, 2000). In addition, the President's Commission on Critical Infrastructure Protection issued its report that same

year and cited “that vulnerabilities were steadily increasing, while the costs of attack were decreasing” (Denning, 2000). With the new computer devices being developed and new software systems being created, vulnerabilities to computer systems will continue to rise.

Computer systems that maintain and operate water and energy resources are particularly vulnerable to terrorist attacks. Computer components that operate these systems are susceptible to intrusion attacks. Critical components of a computer consist of the hardware and software systems.

HARDWARE

Hardware failure can occur due to data error and/or software programming. In addition, computer hardware systems should be protected from fires, extreme temperatures, and humidity (Laudon and Laudon, 2002, page 442). The hardware system contains 6 major components:

1. Central Processing Unit (CPU)
2. Input Devices (keyboard, computer mouse, touch screen…etc…)
3. Output Devices (printers, plotters, audio output, etc.)
4. Primary Storage
5. Secondary Storage (magnetic disk, optical disk, magnetic tape)
6. Communication Devices (Laudon and Laudon, 2003, page 143)

These components are the skeleton that enables a computer to run its programs and/or applications. These are some of the areas where processing errors may occur and cause the hardware components to fail. An example of a potentially hazardous element to a computer would be electricity. Electricity is prone to surge in outlets and can cause vast damage to computer systems. Many power supplies to computer desktops have been fried due to these surges.

SOFTWARE

According to Laudon and Laudon (2002 p. 438), there are two major types of software systems: system software and application software. Each provides communication links to perform functions and act as intermediary between stored information and programs. Each component of the hardware and software system can be affected by product failures or compatibilities issues. Preventing such failures is essential in the operations of infrastructures that are linked to computer systems. An example of software failure can be seen in the Operation of Desert Storm. On February 25, 1991, a patriot missile defense system operating at Dharan, Saudi Arabia failed to intercept incoming Scud missiles because of a software error in the system's weapons control computer. The scud attack killed 28 American soldiers in an army barrack.

In another related issue, Microsoft issued a security warning to its customers citing "serious security problems with its Windows software that could let hackers break into their computers to steal files, delete data or eaves drop on sensitive information." Microsoft indicated it was unaware of any systems being affected. The company offered a patch on its website to correct this security lapse. (*Austin American-Statesman*, *Business Digest*, February 2004)

Updating software and hardware structures are essential to minimize threats. Patches and updates for these systems can be gained from the Justice Department's National Infrastructure Protection Center bi-weekly publication, "Cybernotes". This publication outlines software bugs and provides patches to fix a problem.[6]

[6] The website for viewing this summary is:www.nipc.gov/cybernotes/vcybernote.htm. (National Infrastructure Protection Center, Cybernotes) For Microsoft users, Microsoft provides free software updates on their website at www.microsoft.com.

In his article, Andy Krupa (2002) outlines some security measures in contingency planning. He indicates that "it is extremely difficult to keep up on the latest vulnerabilities, viruses, patches, trends, technology, hacker behaviors and activity." Computer systems have vulnerabilities where hackers, viruses, Trojan horses, and worms can conspicuously destroy and alter information within a computer system, causing damage and disrupting services.

Threats to the software and hardware systems include intrusion by hackers, viruses, worms, and Trojan horse. The following section provides a detail look at each threat.

HACKING

The National White Collar Crime Center (NWCCC) defines hacking as "unauthorized access with malicious intent – to cause damage, steal property (data or services), or simply leave behind some evidence of a successful break-in" (NWCCC, 2003). A hacker is "a person who gains unauthorized access to a computer network for profit, criminal mischief, or personal pleasure" (Laundon and Laundon, 2002, p.435). Infiltration of the computer system can occur within the organization or breached from the outside in the cases of hacking. Hacking can be defined as "the intentional penetration of an organization's computer system, accomplished by bypassing the system's access security control" (Gelinas and Sutton, 2002, p. 265). Some hackers can infiltrate a system and merely look within the system and not harm the companies' information system. Whereas, other hackers have been known to disrupt the computer system and steal proprietary information.

In March 2003, a computer hacker infiltrated the University of Texas computer systems and stole social security numbers of approximately 59,000 current and former students (Haurwitz, 2003). This type of information poses fertile ground for identity theft. Hackers may steal credit card accounts and/or social security numbers to get credit information on an unsuspecting individual. Another malicious avenue is a computer virus. Hackers penetrate network systems to implant a virus into a business' computer system in order to disrupt services.

VIRUSES

The National White Collar Crime Center defines a virus as "a computer program designed to 'infect' a program file or boot sector of a computer. Like a biological virus, a computer virus infects (or copies code to) a 'host' and uses the capabilities of its host to replicate" (NWCCC, 2003). Viruses can damage an information system from other computers via e-mail, "infected" disks or other computer machines. "Mobile device viruses can pose a serious threat to an enterprise computer because so many wireless devices are now linked to corporate information systems" (Laudon and Laudon, 2002, p.436).

Viruses have cost millions of dollars in damages to businesses. Disruption in services can claim millions of dollars in business revenue loss. Corporations, governments and private citizens use antivirus software to combat these viruses. Some viruses can infect a computer system despite their systems having antivirus software, because the user does not update the software. Combating these viruses can be as simple as being keenly aware of the newest threats. Usually, the news media and computer companies inform the public of any new viruses that appear on computer systems.

Laudon and Laudon (2002, p.436) lists a few examples of computer viruses:

- "Concept, Melissa: Macro viruses that exist inside executable programs called macros, which provide functions within programs such as Microsoft Word. Can be spread when Word documents are attached to e-mail. Can copy form one document to another and delete files.
- Form: Makes a clinking sound with each key stroke but only on the eighteenth day of the month. May corrupt data on the floppy disks it infects.
- Explore.exe: "Worm" type virus that arrives attached to e-mail. When launched tries to e-mail itself to other PCs and to destroy certain Microsoft Office and programmer files.
- Monkey: Makes the hard disk seem as if it has failed, because Windows will not run.
- Chernobyl: Erases a computer's hard drive and ROM BIOS (Basic Input/Output System).
- Junkie: A "multipartite" virus that can infect files as well as the boot sector of the hard drive (the section of a PC hard drive that the PC first reads when it boots up). May cause memory conflicts."

Unlike a virus, a worm is self-executing; it does not require a host to replicate" (NWCCC, 2003).

WORM

The National White Collar Crime Center defines a worm as "a computer program designed to make copies of itself" (NWCCC, 2003). Computer worms are "reproducing programs that run independently and travel across network connection" (Virus or Hoax, 2004[7]). Difference between viruses and worms are mode of infection and replication. "A virus is dependant upon a host file or boot sector and the transfer of files between machines to spread, while a worm can run completely independently and spread of its own will through network connections" (Virus or Hoax, 2004). Viruses infect non-mobile files and require users' action to active the virus (Weaver, Paxson, Staniford,

[7] Virus or Hoax? is a website that provides information on viruses, hoaxes, Trojan horses, macro viruses, worms and email bombs. www.virusall.com/index.html

Cunningham, 2003). The worm can distribute itself in various manners. The following are different ways that worms can spread:

- "Self Carried: A self-carried worm actively transmits itself as part of the infection process.
- Second Channel: Some worms, such as Blaster [31], require a secondary communication channel to complete the infection.
- Embedded: An embedded worm sends itself along as part of a normal communication channel, either appending to or replacing normal messages" (Weaver, Paxons, Staniford, Cunningham, 2003)

Unlike the worm, the Trojan horse is concealed within a program and acts like a time bomb.

TROJAN HORSE

The National White Collar Crime Center defines a Trojan horse as "a program that appears to be useful or benign but actually conceals a smaller program that is designed to be damaging" (NWCCC, 2003). A Trojan horse is a hidden program that "sleeps" until some specific event occurs, activating the program (Turban, McLean, Wetherbe, 2002, p. 672). A Trojan horse infects a computer whenever a user clicks on an e-mail attachment, downloads a file, or installs it physically with an infected medium (disk, zip file,) (Zetter, 2002). Firewall protection is usually one measure to detect a Trojan horse. With new advances in technology, new viruses and Trojan horses are finding new ways to penetrate a computer system.

At a Def Con Convention[8], three South African researchers demonstrated a Trojan horse, "Setiri" that bypassed a firewall detection system using Microsoft's Internet Explorer window IEXPLORE.EXE (Zetter, 2002). Setiri launches an invisible window in Internet Explorer to connect to a Web server through an anonymous proxy site. Setiri uses this site to execute commands on PC without users' knowledge. "The Trojan horse

[8] **DEF CON** Computer Underground Hackers Convention Index Page www.defcon.org, April 2004

exploits a standard feature in Internet Explorer that lets invisible browser windows open and connect to the Internet. The browser windows open in the background and don't appear on the desktop, so you can't see what they're doing. If you look for evidence of an open window in your Window Task Manager, the window will be listed as IEXPLORE.EXE, just like a regular Internet Explorer window….Internet Explorer uses invisible windows for many legitimate purposes such as sending registration information to the Net" (Zetter, 2002).

Unlike Seitiri, a new Trojan horse, "Phatbot" has emerged and has security expert fearful of its impact. U.S. Department of Homeland Security issued an alert to select group of computer security experts regarding "Phatbot" during the week of March 8, 2004. Phatbot uses the peer-to-peer (P2P) networking system and this concerns officials. "The concern here is that the P2P like characteristics of these [Phat]'bot networks may make them more resilient and more difficult to shut down," said a cyber-security official at the Department of Homeland Security" (Krebs, 2004). Phatbot "allows its authors to gain control over computers and link them into P2P networks that can be used to send large amounts of spam e-mail messages or to flood Web sites with data in an attempt to knock them offline" (Krebs, 2004).

According to this article, an antivirus product can detect Phatbot, but as soon as the Trojan horse infects computers, it disables many antivirus and firewall software tools. Phatbot authors can use this Trojan horse in a denial of service attack, but is limited because according to Lurhq's Stewart the "Trojan is designed to link computers into groups no larger than 50 computers, which would significantly limit the Trojan's effectiveness as a denial-of-service tool" (Krebs, 2004).

DENIAL OF SERVICE (DoS) ATTACK

The National White Collar Crime Center defines a denial of service attack as "an explicit effort to prevent legitimate users from accessing computer systems" (NWCCC, 2003). In a denial of service attack, "a web site is overwhelmed by an intentional onslaught of thousands of simultaneous messages, making it impossible for the attacked site to engage in its normal activities. A distributed denial of service attack uses many computers (called "zombies") that unwittingly cooperate in a denial of service attack by sending messages to the target web site" (Gelinas and Sutton, 2002, p. 261).

In February 2000, due to the denial of service attack, Yahoo was unavailable for three hours; Amazon was down for an hour. They lost $500,000 and $240,000 respectively (Gelinas and Sutton, 2002, p. 261). According to Gelinas and Sutton (2002, p.261), remedies against this sort of infiltration is to detect these attacks and use filters to detect the messages, block traffic from the site sending them and switch legitimate message to Internet Service Providers that are not under attack. They recommend carrying insurance to safeguard against costs associated with this intrusion.

When a computer system crashes, continuous service is disrupted; a disaster recovery plan would enable corporations to rapidly recovery data information and conduct business. A denial of service attack would provide hackers an avenue to disrupt the services of business and provide a distraction while other criminal activities are taking place. If someone is trying to penetrate a secured building, a hacker could use this method to crash the computer systems, thereby having individuals penetrate the facilities when the systems are down.

Michael Vatis, former head of NIPC told the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations “the possibility is there to take down significant portions of the Internet and the critical infrastructures that rely on the Internet” (Thibodeau, 2001). Vatis’ prediction become a reality on October 23, 2003 when 9 of the 13 computer servers that manage global Internet traffic were attacked by a denial of service attack and where momentarily disabled (Associated Press, October 23, 2002).

SUMMARY OF CYBER THREATS

Each of above mentioned cyber threats can essentially shut down servers and systems thereby causing disruptions in computer systems of water and energy infrastructures. By taking precaution measures, security experts can protect computer systems from harmful attacks.

The National Infrastructure Protection Center, based at FBI headquarters was formed in 1998 to handle threat assessments, investigations and responses to any attacks on critical U.S. infrastructures (Thibodueau, 2001).

Security Measures and Studies

Security experts predict that not all businesses are taking these warning seriously. “The risk of the typical U.S. company suffering at least one major cyberattack within the next year is strong, and not enough businesses are taking appropriate steps to defend themselves”, according to the results of a survey released Wednesday by the Business Software Alliance (BSA) (Krazit, 2002). "This report is a wake-up call for the private sector; they have as much to be concerned about as the public sector," said U.S.

Representative Billy Tauzin, a Republican from Louisiana. "The strength of the American economy depends on making our infrastructure safe," according to Tauzin. Businesses are apprehensive about reporting incursion of their system for fear of bad publicity and loss of confidence by the public.

The Director, CERT Coordination Center[9], speculated that 80 percent of actual security incidents go unreported in most cases because (1) the organization was unable to recognize that its systems had been penetrated or there were no indications of penetration or attacks, or (2) the organization was reluctant to report (GAO 03-233, p. 7).

In an April 2002 report of the Computer Crime and Security Survey, 90 percent of respondents (primarily large corporations and government agencies) had detected computer security breaches (GAO 03-233 report cites Computer Security Institute[10]). Robert Holleyman, Vice President of BSA, states "Most attacks are never reported, and we need to examine the attacks and look for patterns that will allow authorities to locate the attackers….We need to create incentives for companies to report vulnerabilities and incursions to their networks without the fear of that information being released to competitors" (Krazit, 2002).

Since September 11, 2001, ASIS International employment survey, conducted by Westat, Inc. focused on what companies have done since the September 11, 2001, terrorist attacks on the WTC and the Pentagon. Security Management interviewed

[9] Established in 1988, the CERT® Coordination Center (CERT/CC) is a center of Internet security expertise, located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University. (http://www.cert.org/)

[10] Computer Security Institute, "2002 Computer Crime and Security Survey," *Computer Security Issues & Trends*, volume VIII, No1, Spring 2002

security administrators to assess specific changes in their companies. Additional perspectives were gathered from security suppliers at the ASIS 48th Annual Seminar and Exhibits in Philadelphia (Anderson, 2003, p. 62). In this survey, 74 percent of those surveyed experienced "no change in the security function's structure within the organization as a result of 9-11". However, 18 percent of respondents said that security now reports to a person with a higher rank, and 7 percent said the security department is structured under a different department (Anderson, 2003, p. 62). In addition, policy changes were most cited in response to 9-11 (Anderson, 2003, p. 64).

According to one respondent, Charles R. Schobee chief of security for the Landings Association, Savannah, GA developed several plans for his company. He devised an emergency preparedness plan for the community that addressed explosions, chemical agents, and suspicious packages. A threat assessment revealed potential vulnerabilities where water supply sources were not checked by security. Now, Mr. Schobee has each water well checked regularly by security guards (Anderson, 2003, p. 64).

While some security experts reported increases in security awareness and improvement since September 11, 2001, others have reported companies not making the necessary security measures. In a recent Council on Competitiveness survey of 230 corporate executives, 67 percent of the respondents "failed to see how enhanced security could make them more economically competitive" (Harowitz, 2003, p. 57). In this same survey, respondents did not see their companies as targets of terrorism. Though 70 percent of their companies had reviewed and discussed security polices and 53 percent had made changes based on those assessments (Harowitz, 2003, p. 58).

Further studies include one cited in Security Management's news and trends article indicated a small sample of firms studied by the U.S. General Accounting office indicated September 11th incident did not alter employee-computer-use policies.

Moreover, GAO examined the practices of 14 Fortune 1000 companies, and found that none had changed computer practices and policies due to September 11 and it's aftermath (Security Management, p. 25). It is those companies that are securing their facilities and computer systems, that will have a business advantage over those companies that are not outlining risk assessment for such attacks.

PHYSICAL THREATS

On September 11, 2001, terrorists used airplanes to destroy the Word Trade Center Financial District. Physically destroying a symbolic asset provided a desirable effect for terrorism: Fear; fully halting the U.S. economy. The financial and economical nerve of the U.S. was disrupted. The Twin Towers were destroyed. Critical infrastructures can be physically attacked via bombs and incendiaries that result in fire damage, water damage, and power loss (CACI, International, Inc., February 11, 2004). Securing the physical structure of the infrastructure is essential. Securing the physical perimeters of critical infrastructures could safeguard and diminish the probability of tampering and damaging the infrastructures.

FIRE DAMAGE

Fire damage is an environmental factor that can destroy valuable information and structures that lie in its wake. Computer components are sensitive to this environmental factor. Hardware systems are sensitive to heat. Fans are usually found connected to the mother boards to cool elements within the system. Buildings or structures that house

infrastructure systems are vulnerable to this factor. Proactive measures include, smoke detectors, fire alarms, fire extinguishers, fire resistance material, insurance and firewalls (Gelinas and Sutton, 2002, p. 266).

WATER DAMAGE

Flooding is another environmental factor that can destroy valuable information and structures. Water and electronic components are incompatible. Electronic components usually short if submerged in water. Broken water pipes can result in damaged computer systems and structures. Per Gelinas and Sutton (2002, p. 266), proactive measures in preventing water damage includes: "waterproof ceilings, walls, and floors; adequate drainage; water and moisture detection alarms; and insurance."

DISRUPTION – Power Loss

Disruption in electricity can prove costly. Computer systems are down and information contained in the systems are not readily available to assist customers or provide electricity or water to customers.

Brownout can cause damage to computers systems and electronic systems. Brownouts are "periods of low voltage in utility lines that can cause lights to dim and equipment to fail. Also known as voltage sag, this is the most common power problem, accounting for up to 87% of all power disturbances" (IBM UPS Systems, 2004). According to IBM, brownouts places undue straining power equipments and destroying electrical component that causes hardware failure. Preventative measures for brownouts include using UPS systems. UPS systems control "voltage by switching over to battery power when line voltages move beyond preset limits" (IBM UPS Systems, 2004).

Gelinas and Sutton (2002, p. 266) recommend voltage regulators, backup batteries and generators.

Blackouts are power failures. Failure in the power grids caused the massive blackout in the Northeast in August 2003. Again backup systems, such as generators, batteries and UPS systems are some preventative measures in not losing valuable information and disruption of services.

Physical threats to water systems include contaminants in the water source supply. These contaminants could include biological, chemical and radiological substances that would make water sources useless. Pipelines that distribute water to businesses and homes can have breaks, thereby disrupting services. Mr. Arnaud de Borchgrave, terrorism expert, indicated that water seemed to be the main target of these cyber-intelligence-gather efforts (Harris, 2002, p. 36).

In its report, GAO (GAO-04-29, 2003) cited "distribution systems as among the most vulnerable physical components of a drink water utility." In this report, experts identified two vulnerabilities: "a lack of information individual utilities need to identify their most serious threats; and (2) a lack of redundancy in vital system components, which increases the likelihood that an attack could render an entire utility inoperable" (GAO-04-29, 2003). The GAO recommended that U.S. Environmental Protection Agency enhance its effort in assisting drinking water utilities to reduce their vulnerabilities to terrorist attacks by allocating security-related fund to these facilities (GAO-04-29, 2003). The GAO cites physical disruption, bioterrorism, chemical contamination, and cyber attacks as threats to drinking water facilities.

BIOLOGICAL THREAT

A biological attack is defined as "the deliberate release of germs or other biological substances that can make you sick" (US DHS, Ready.gov, 2004). The Department of Homeland Security includes, anthrax, smallpox and virus that can potential cause serious bodily harm or death. These agents can be deliberately introduced into hosts who transmit them to unsuspecting population.

CHEMICAL

A chemical attack is defined as "the deliberate release of a toxic gas, liquid, or solid that can poison people and the environment" (US DHS, Ready.gov, 2004). Nerve gases, acids, and/or mercury poisoning are some examples of these types of agents. The Toyko subway Sarin nerve gas attack is one example of a terrorist act that killed 12 innocent people in 1995 (Pangi, 2002).

RADIOLOGICAL

A radiation threat, "commonly referred to as a 'dirty bomb' or 'radiological dispersion device (RDD)', is the use of common explosives to spread radioactive materials over a targeted area" (US DHS, Ready.gov, 2004). According to the DHS website, DHS recommends limiting your exposure and avoid breathing radiological dust.

TEXAS DEPARTMENT OF HEALTH

Texas Department of Health (TDH) is the lead liaison for bioterrorism, chemical and radiological attacks in Texas. TDH has various advisory committees including Bioterrorism Preparedness and Response Committee, Preparedness Coordinating Council and Bureau of Emergency Management to address the needs of these types of attacks. Within the Preparedness Coordinating Councils, 17 various agencies, including the Texas

Regional Councils of Government help coordinate assistance in case of emergencies (Texas Department of Health, 2004).

AREAS OF CONCERN FOR WATER AND ELECTRICITY SECTOR

According to the *Strategy* there are four areas of focus for the water sector: (1) Physical damage or destruction of critical assets, including intentional release of toxic chemicals; (2) Actual or threatened contamination of the water supply; (3) Cyber attack on information management systems or other electronic systems; and (4) Interruption of services from another infrastructure (Strategy, 2003, p. 39). Restricting physical access to these structures and computer facilities and control access within the structures themselves are ways to diminish vulnerabilities. Early warning of the contamination of a water supply is essential in order to relay this information to the public.

The *Strategy* identifies the physical components for the electricity sector; they include: (1) Generation; (2) Transmission and distribution, (manage and control the distribution of electricity) and (3) Control and communication (operate and monitor critical infrastructure components) (Strategy, 2003, page 50). Identifying these components can dictate what would be considered physical threats to this infrastructure.

Security Measures

There are various security measures that can be employed to protect the facilities that operate and maintain our infrastructures. Restricting access to and/or around the infrastructure provides a solution to security threats. The physical perimeters of these facilities can have security gates and fences placed to provide limited access. Armed personnel can be employed to guard certain key entrances around a facility. Security

cameras can be placed around the facility to monitor the entrances and activities throughout the facility. Sign in sheets can be used to determine an individual's presence in the buildings. Security badges can limit access for employees and limit entrance to a secured room.

Once the perimeters of building are secured, the computer systems within the buildings should be fortified from intrusions. Companies can develop policies and guidelines in computer usage. Passwords, encryption software, firewall, routers, security electronic badges and/or monitors can be implemented to safeguard the systems from intrusions. These are some of the security measures mentioned in the literature review that preserve computer systems within facilities.

In his article, "*The Oversights of Physical Security and Contingency Planning*", Andy Krupa emphasizes access control and physical security in addition to computer security measures such as firewalls, and intrusion detection systems. According to his article, Price Waterhouse Coopers is quoted as stating "90 percent of all companies that experience a computer 'disaster' with no pre-existing survival plan go out of business within 18 months." According to Krupa, a "lack of contingency planning in the case of a disaster (whether it be flood, fire or theft) will lead to a loss of functionality, time, resources and perhaps more importantly a loss of service that the data systems provide."

After identification of these vulnerabilities is established, fixing these vulnerabilities is the next step. Developing procedures and establishing a time interval for periodical testing of these vulnerabilities is essential. New methods for penetrating the computer systems are developed on an ongoing basis. By testing periodically, new vulnerabilities can be identified and fixed.

DISASTER RECOVERY PLAN

The disaster recovery plan is designed to provide continuity of business should a disaster occur such as September 11th. The resumption of business after a devastating event is essential. Time and money are lost every minute that a business is disrupted Monies are lost if data and information are lost. Planning, updating systems policies and procedures prove critical in providing services where the disaster occurs. According to Gelinas and Sutton, a contingency plan should include: the physical computer facilities, computer, equipment (communications, fax, phone lines and/or vital equipment in the event of a disaster), supplies and personnel.

MIRROR SITE

The authors advocate that corporation needing immediate business resumption "should incur the cost to maintain two or more sites; primary site and a mirror site that maintains copies of the primary site's programs and data" (Gelinas and Sutton, 2002, page 259). Mirroring uses "a backup server that duplicates all the processes and transactions of the primary server. If the primary server fails, the backup server can immediately take its place without any interruption in service" (Laudon and Laudon, 2002, p. 445). This type of mirroring may prove costly. Less costly of an alternative plan is to transmit pertinent data on a continuous basis to an off-site electronic vault. Unlike the mirroring, this would not automatically take over should the primary facility become incapacitated (Gelinas and Sutton, 2002, page 259).

Clustering is "a less expensive technique for ensuring continued availability. High-availability clustering links two computers together so that the second computer can act as a backup to the primary computer. If the primary computer fails, the second

computer picks up its processing without any pause in the system" (Laudon and Laudon, 2002, p. 445).

Still other arrangements could facilitate the corporation by contracting with disaster recovery contractors, namely hot sites and cold sites.

HOT SITES

Hot sites are fully equipped data centers, often housed in bunker-like facilities that are made available to corporations for a monthly fee. Hot sites are a second venue where most corporations can take their backup data information and continue their production on site. It is an alternative location that enables the corporations to continue operating until a more permanent solution is provided. Hot sites enabled a Singapore-based Overseas Union Bank, housed on the 39th floor of the World Trade Center to mobilize their disaster recovery plan and minimize business interruption (Turban, McLean and Wetherbe, 2002, p. 717). Hot sites are more expensive than cold sites, because most of the infrastructure and computer systems are ready for use. Hot sites seem more suitable for infrastructures, such as the government, that would protect themselves from nuclear disasters.

COLD SITES

Cold sites are air conditioned elevated places that can have computer workstations to operate on any given notice, like 18-wheeler trucks for mobility (Gelinas and Sutton, 2002, p. 259). Cold sites could feasibly be used for insurance companies that have to evaluate disaster areas affected by hurricanes, tornadoes, and/or floods. This method provides mobility to the insurance corporation so that they can expedited claims and payments to help the area rebuild.

In developing a contingency plan, all key personnel need to be involved in its construction. Water and energy infrastructures have both private entities and government agencies involve in providing services to the public. Therefore, it is crucial for key personnel from private and public entities to share pertinent information to safeguard these sectors.

According to Scott Hanning in "*Recovering from Disaster: Implementing Disaster Recovery Plans Following Terrorism*," he specifies three conditions in a disaster recovery proven to be challenging for companies. They are:

- Accessing the needed software and technology
- Staying connected with employees and customers
- Loss of valuable personnel

Hanning advocates current recovery policies for organizations and periodic reviews and updates. Additionally, Hanning contends that backup logs should be kept and critical information residing on the computers should be backed up on a regular basis. Per Hanning, "Full daily backups or online disk storage may not be as necessary per se [as] mission critical systems or applications, but should be backed up incrementally, either daily or weekly, as is appropriate for business needs. In the event of a disaster, the unavailability of backup tapes may significantly affect restoration activities. Redundancy such as this is what saved many of the businesses affected by the September 11 terrorist attacks." Included in Hannings' article, was a summary of recommendations that analyst from Gartner Inc. outlined for the re-evaluation of disaster recovery plans in a report by Nancy Weil:

- Get alternate email addresses for employees

- Distribute "wallet cards" with information about what to do in case of an emergency
- Create a designated place for evacuated employees to assemble in the case of a disaster
- Include local, state, and federal employees in disaster recovery planning

In his article Andy Krupa, (2002) suggests formulating a response team and developing a contingency plan that would include mirroring. He also recommends conducting monthly or quarterly test on alarm systems and emergency power systems. Mr. Krupa further suggests keeping copies of crucial documents.

In assessing these contingency plans, the resounding message is to plan for a disaster. Planning and assessing the weak areas of access and physical security are essential in drafting a contingency plan. Draft policies and procedures on these security measures and provide copies to appropriate staff. Employees should be well versed on these polices and procedures and informed that they are accountable for these policies being enforced.

In developing a contingency plan, all key personnel need to be involved in its construction. Water and energy infrastructures have both private entities and government agencies involve in providing services to the public. Therefore, it is crucial for key personnel from private and public entities to share pertinent information to safeguard these sectors.

INFORMATION SHARING

According to Thomas R. Davies, most industries are responsible for part of the country's critical infrastructures: gas and electric, have been assessing vulnerabilities, developing plans, implementing procedures and taking measures in protecting their

infrastructures (Davies, 2001). Davies states that state and local governments have not kept up and are least a year behind due to the structure of the government and cited "fragmentation of state and local government acts as barriers" to the coordinated efforts. Davies cites conflicts within state and local government inhibit coordinating efforts. For instance, law enforcement agencies struggle to share access to sensitive intelligence concerning investigations with those inside and outside the law enforcement community.

Information Sharing and Analysis Centers

According to Matthew Devost (2002, p.35), information sharing and remediation strategies between the public and private sector should be addressed at the state and federal level. Devost recommends that federal, state, and local governments should be talking with private sector and sharing information.

The *Strategy* emphasizes this component in its literature and Devost repeats this idea in his literature. This literature provides the information sharing vulnerability component in the conceptual framework for this applied research project.

Coordination is the key function in protecting our critical infrastructures. "Protecting critical infrastructures and key assets will require a particularly close and well-organized partnership among all levels of government" (Strategy, 2003, p. 19). The Strategy encourages the partnership of all levels of government and private entities. Presidential Decision Directive (PDD) 63 on Critical Infrastructure Protection encouraged the development of the Information Sharing and Analysis Center (ISAC) (Bennett, 2002, p. 6). These centers encouraged coordination between owners and operators to facilitate an information sharing systems within the private sector.

Exchanges of potential threats, vulnerabilities, risk assessments and solution are pondered.

ISAC are currently found in the electricity and water sectors. The Water ISAC coordinates with Environmental Protection Agency and other federal agencies to share information regarding contamination threats such as the release of biological, chemical and radiological substances in to the water supply and how to respond to their presence in drinking water (Strategy, 2003, p. 39).

North American Electric Reliability Council (NERC) is a nonprofit corporation made up of 10 regional councils in the United States and Canada. Members of these councils include all segments of the electricity industry (Strategy, 2003, p. 50). NERC serves as one of the ISAC to which security measures and alert systems are developed. The electricity sector engages in daily communications between the federal government and electric grid operators around the country (Strategy, 2003, p. 51).

Each component of the literature stress key concerns on public infrastructures. These concerns, computer vulnerabilities and physical threats, demonstrate a need to be identified and addressed to ensure protection. These components are highlighted in the conceptual framework.

Conceptual Framework

The conceptual framework for this research project will be descriptive in nature. Descriptive categories will be used to identify the critical infrastructures and their vulnerabilities within computer systems and physical threats. Categories are the easiest and most basic conceptual framework to see/use (Shields, 1998, p. 59). Two critical infrastructures were selected from the 16 infrastructures identified by the Department of

Homeland Security: Water and Energy (Fresh water supply and Electricity). These two resources will be used to evaluate Texas Regional Councils' assessment of water and energy systems in their region. For the purpose of this applied research project, fresh water supply and electricity were selected from these sectors to limit scope of this research.

In addition to identifying the critical infrastructures, the critical infrastructure vulnerabilities are categorized in two sections: computer-related vulnerabilities and physical threats. A list of security measures was identified through an examination of the literature review that addressed both computer-related and physical security vulnerabilities. The literature review provided various models and suggestions on how to fortify computer systems and the physical structures of critical infrastructures. Among these literatures are documents drafted by the Department of Homeland Security which provides proactive approaches in ensuring the security of infrastructures. In addition, disaster recovery was suggested as a secondary method in case the proactive measures did not prevent an aggressive attack on the security systems.

The following are the components to the conceptual framework:

- Computer Vulnerabilities: Hacking, viruses, computer worms, Trojan Horses and denial of attacks;
- Physical Threats: Destruction, disruption of water distribution, fire damage, water damage, power loss, contamination (biological, chemical and radiological), Avert physical threat by restricting access to infrastructures and computer facilities and enforcement of structures.
- Disaster Recovery – Mirroring, Hot Site, Cold Site
- Information Sharing – Between government agencies and private entities and/or among government agencies.

The literature review provides the components to the conceptual framework. The components in the conceptual framework are illustrated in Table 3.4

Conceptual Framework - TABLE 3.3 Type of Framework: Descriptive Categories

Identify Key Assets and/or Infrastructures Infrastructures Examined • Fresh Water Supply[11] • Electricity[12]	The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets2003 The National Strategy to Secure Cyberspace 2003 Texas Natural Resource Conservation Commission, 2001 Texas Public Utility Commission , 2003 Jurst and Tritak, 2002 GAO Report 02-233, 2003 Harris, 2002 Chiruvolu, 2003 Hulme, 2003 ERCOT, 2004
Computer System/Cyber Vulnerabilities	
• Software/Hardware -Hacking -Denial of Attack -Viruses -Trojan Horses -Worms	The National Infrastructure Protection Center, Cybernotes 2002 and 2003 The National Strategy to Secure Cyberspace 2003 Laudon and Laudon, 2002 Government Security 2003 http:/www.ojp.usdoj.gov/funopps.htm Allen 2003, Anderson 2003, Krupa, 2002, Devost 2002, Pangi, 2002, Krazit, 2002 American Statesman, Business Digest, February 2004 Thibodueau, September 2001 National White Collar Crime Center, 2003
Physical Security Threats	
• Physical destruction and/or disruption -Fire Damage -Water Damage, -Power loss • Restrict Access to Infrastructures and computer facilities • Contamination: -Chemical, -Radiological -Biological	The National Strategy to Secure Cyberspace 2003 The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets 2003 Devost, 2002 Government Security 2003 hhtP:/www.ojp.usdoj.ogv/funoops.htm
Disaster Recovery/ Information Sharing	
• Disaster Recovery/Contingency Planning -Mirroring sites -Hot sites -Cold sites • Coordinating Information with levels of government and private entities	Bennett, 2002 CACI, International, Inc. 2002 Davies, 2001 Gelinas and Sutton 2002 Hanning 2001 Krupa 2002 The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets 2003

[11] For purposes of this applied research project, fresh water supply was selected for this sector. Waste water centers are also part of this infrastructure but are not included to limit the scope of this research.
[12] For purposes of this applied research project, electricity was selected for this sector. Oil refineries and gas suppliers are also part of this infrastructure but are not included to limit the scope of this research.

CHAPTER FOUR
METHODOLOGY

INTRODUCTION

The purpose of this research is to assess the Texas water & energy infrastructures vulnerability from the point of view of Texas Regional Council leaders. The key areas of concern are physical security threats and vulnerabilities to computer systems. In addition, opinions regarding disaster recovery and information sharing are reviewed. The purpose of this chapter is to describe the methods enacted in obtaining the data for this applied research project.

SURVEY RESEARCH

Survey research was the method used to gather information to determine the Council leadership's opinions and attitudes on water and electricity vulnerabilities. The survey was developed from the conceptual framework illustrated in Chapter 3. The survey instrument was pre-tested by members of the Homeland Security Program and members of the Special Investigations Unit, State Auditor's Office for sensitivity and response rates. The survey instrument included a letter explaining the nature of this research to provide credibility. Questions regarding the survey were directed to a member of the Texas Domestic Preparedness Program and an academic advisor who substantiated the research.

Opinions and attitudes was the best approach in data collection. Obtaining any other information would prove futile since information regarding public infrastructures' vulnerabilities would be regarded confidential. Due to the nature of this research project,

anonymity would provide the best approach. Revealing information from segments of the state would indicate vulnerabilities in this area and generate risk for that area.

Questionnaire items link the research purpose through the conceptual framework. The research purpose for this applied research project is to assess the Texas water & energy infrastructures vulnerability from the point of view of Texas Regional Council leaders. The key areas of concern are physical security threats and vulnerabilities to computer systems. In addition, opinions regarding disaster recovery and information sharing are reviewed. The conceptual framework was the guide in constructing the survey instrument. Table 4.1 links the survey instrument to the conceptual framework. Table 4.1 illustrates the operationalization of the conceptual framework.

Operationalization of Conceptual Framework – TABLE 4.1

Infrastructures and Vulnerabilities	**Infrastructures Examined** • Fresh Water Supply[13] • Electricity[14]
Computer System/Cyber Vulnerabilities	**SURVEY QUESTIONS**
Software/Hardware -Hacking -Denial of Attack -Viruses -Trojan Horses -Worms	1. Computer systems that operate and/or maintain **water** systems are vulnerable to hacking. 2. Computer systems that operate and/or maintain **water** systems are vulnerable to viruses. 3. Computer systems that operate and/or maintain **water** systems are vulnerable to computer worms. 4. Computer systems that operate and/or maintain **water** systems are vulnerable to Trojan Horses. 5. Computers systems that operate and/or maintain **water** systems are vulnerable to denial of service attacks. 6. Computer systems that operate and/or maintain **water** systems should not be accessible by remote access via modem and/or internet. 17. Computer systems that operate and/or maintain **electricity** are vulnerable to hacking. 18. Computer systems that operate and/or maintain **electricity** are vulnerable to viruses. 19. Computer systems that operate and/or maintain **electricity** are vulnerable to computer worms. 20. Computer systems that operate and/or maintain **electricity** are vulnerable to Trojan Horses. 21. Computers systems that operate and/or maintain **electricity** are vulnerable to denial of service attacks. 22. Computer systems that operate and/or maintain **electricity** should not be accessible by remote access via modem and/or internet.
Physical Security Threats	
• Physical destruction and/or disruption -Fire Damage -Water Damage -Power loss • Restrict Access to Infrastructures and Computer Facilities • Contamination -Chemical -Radiological -Biological	7. Reinforcement of new and/or existing structures is necessary to avert physical threats on **water** systems. 8. Destruction of **water** systems is a concern. 9. Disruption of **water** distribution is a concern. 10. Fire damage to **water** systems is a concern 11. Power loss to **water** systems is a concern. 12. Restricting access to **water** systems are necessary to avert physical threat 13. Restricting access to buildings and computer systems are necessary to avert physical threats to **water** systems. 14. Chemical contamination of **water** systems is a concern. 15. Radiological contamination of **water** systems is a concern. 16. Biological contamination of **water** systems is a concern 23. Reinforcement of new and/or existing structures is necessary to avert physical threats on **electricity** supply system. 24. Destruction of **electric** supply system is a concern. 25. Disruption of **electricity** supply system is a concern. 26. Fire damage to **electricity** supply system is a concern. 27. Water damage to **electricity** power system is a concern. 28. Restricting access to **electricity** supply systems is necessary to avert physical threat. 29. Restricting access to buildings and computer systems is necessary to avert physical threats to **electrical** grid and power supply

[13] For purposes of this applied research project, fresh water supply was selected for this sector. Waste water centers are also part of this infrastructure but are not included to limit the scope of this research.

[14] For purposes of this applied research project, electricity was selected for this sector. Oil refineries and gas suppliers are also part of this infrastructure but are not included to limit the scope of this research.

Operationalization of Conceptual Framework – TABLE 4.1 – Continued

Disaster Recovery/ Information Sharing	**SURVEY QUESTIONS**
• Disaster Recovery/Contingency Planning -Mirroring sites -Hot sites -Cold sites • Coordinating Information with levels of government and private entities	30. Mirroring disaster recovery planning methods for **water** are well developed in Texas local government. 31. Hot site disaster recovery planning methods for **water** are well developed in Texas local government. 32. Cold site disaster recovery planning methods for **water** are well developed in Texas local governments. 33. **Water** disaster recovery planning in Texas local government is satisfactory. 34. Sharing information regarding security measures and disaster recovery planning of **water** infrastructures among local, state and federal government entities is satisfactory. 35. Texas local governments and private entities that own and/or operate **water** critical infrastructures share information regarding security measures and disaster recovery planning on a satisfactory level. 36. Mirroring disaster recovery planning methods for **electricity** are well developed in Texas local government. 37. Hot site disaster recovery planning methods for **electricity** are well developed in Texas local government. 38. Cold site disaster recovery planning methods for **electricity** are well developed in Texas local governments. 39. **Electricity** disaster recovery planning in Texas local government is satisfactory. 40. Sharing information regarding security measures and disaster recovery planning of **electricity** infrastructures among local, state, and federal government entities is satisfactory. 41. Texas local governments and private entities that own and/or operate **electricity** critical infrastructures share information regarding security measures and disaster recovery planning on a satisfactory level.

CODING

Each Council was assigned an alphabetical letter and their response was coded accordingly. A Likert Scale was utilized to evaluate the level of concerns regarding the various vulnerabilities of water and energy infrastructures. The surveys elicit response categories of Strongly Agreed, Agreed, Neutral, Disagreed and Strongly Disagreed. The following numbers were assigned to calculate the responses.

- Strongly Agree = 5
- Agreed = 4
- Neutral = 3
- Disagreed = 2
- Strongly Disagreed = 1

The Result Chapter summarized the various concerns for the physical threats and cyber vulnerabilities. A Likert Scale was utilized in this section to show the degree of concern. The following illustrates these responses:

- Strongly Agree = Very High
- Agree = High
- Neutral = Moderate
- Disagree = Low
- Strongly Disagree = Very Low

STRENGTHS AND WEAKNESSES

The methodology used to obtain data for this applied research project was surveys. According to Babbie, survey research is probably the best method available to the social research who is interested in collecting original data for describing a population too large to observe directly (Babbie, 2001 p. 238). In addition, survey research was utlized because "surveys are also excellent vehicles for measuring attitudes and orientations in a large population" (Babbie, 2001, p.238).

On the other hand, survey research has several weaknesses whereby "survey research is generally weak on validity and strong on reliability (Babbie, 2001, p. 269). Though, this survey provides consistency due to the Likert Scaling. This does not mean that respondents answer the questions wholeheartedly. They may answer in a pattern and may not accurately measure their attitudes (Babbie, 2001.p. 248). Due to the subject matter for this applied research project, these answers may not reflect the entire Texas region as whole. One individual is responding for the Regional Councils may not truly reflect that region.

The drawback to this method is the time constraint and a weak response rate due to the nature of this research. Regional Councils may not respond to this survey due to the sensitive nature of the subject matter: vulnerabilities of water systems and energy systems in their region. By asking for their perceptions and opinions on the subject matter, they may be more inclined to provide information, thereby increasing the response rate.

These surveys did not elicit information regarding the identification of respondents and/or geographical regions. Anonymity obtains a higher response rate. In addition, the survey instrument was pre-tested by members of the Homeland Security Program and members of the Special Investigations Unit, State Auditor's Office for sensitivity and response rates. The survey instrument included a letter explaining the nature of this research to provide credibility. Questions regarding the survey were directed to a member of the Texas Domestic Preparedness Program and an academic advisor who substantiated the research.

Time constraints posed a problem in the response rate. Respondents were limited because of time constraints on their jobs. The survey instrument was developed so that respondents could opine on the statements and return the survey via e-mail to expedite the response. A second survey was provided as a follow up to increase the response rate in this method.

SAMPLE

A survey was sent to coordinators of the twenty-four Texas Regional Councils of Government. There are 24 Regional Councils of Governments that are part of the Texas Homeland Security Program (Texas Engineering Extension Services, 2004). Regional Councils are defined by law as political subdivisions of state, but they have no regulatory power or other authority possessed by cities, counties or other local governments according to Texas Association of Regional Councils (Texas Association of Regional Councils, 2004). The surveys were addressed to staff coordinators within each Regional Council.[15]

A preliminary contact to the Councils via telephone was initiated on March 3 and 4, 2004. The purpose of the calls was to explain purpose of the research, reassure the respondents that anonymity would be respected, and that a survey instrument would be addressed to their attention. These respondents are extremely active in their jobs. Therefore, if there was no response to this initial call, the next individual on the list was contacted. All of the Councils were contacted except one, where a message was left for

[15] This information was gained through the Texas Association of Regional Councils' web site at http://www.txregionalcouncil.org. The website specified each regional section of the state and their respective Councils. The Councils represented surround counties and municipalities which covers the entire State of Texas. Verification was sought through a reliable source. A map of these Councils is attached and can be seen in Appendix A

this particular Council. E-mail surveys were sent on March 3 and 4, 2004 (See Appendix B).

Coordinators, who did not respond, were contacted on March 16 and 17, 2004 via telephone. A deadline of March 20, 2004 was communicated to these respondents. A second e-mail with the survey attached was sent on March 16 and 17, 2004 (Appendix B-1).

COMPOSITE SAMPLE ELEMENT

One representative from each of the twenty-four Councils was expected to respond. Several councils copied the questionnaire and gave it to several coordinators. In order to keep a consistent unit of analysis (one response per Council) composite respondents were constructed using the mode. Table 4.1 illustrates how the mode was calculated for one Council.

COMPOSITE RESPONSE – TABLE 4.2

Questions	COG X	COG X	COG X	Score	Score	Score	Mode
1	Agree	Agree	Agree	4	4	4	Agree
2	Agree	Agree	Agree	4	4	4	Agree
3	Agree	Agree	Agree	4	4	4	Agree
4	Agree	Agree	Agree	4	4	4	Agree
5	Agree	Agree	Neutral	4	4	3	Agree
6	Strongly Agree	Disagree	Disagree	5	2	2	Disagree
7	Agree	Neutral	Agree	4	3	4	Agree
8	Agree	Agree	Neutral	4	4	3	Agree
9	Agree	Agree	Neutral	4	4	3	Agree
10	Agree	Agree	Agree	4	4	4	Agree

STATISTICS

The responses are analyzed using simple descriptive statistics (frequency distributions and mode).

CHAPTER FIVE
RESULTS

INTRODUCTION

The purpose of this research is to assess the Texas water & energy infrastructures vulnerability from the point of view of Texas Regional Council leaders. The key areas of concern are physical security threats and vulnerabilities to computer systems. In addition, opinions regarding disaster recovery and information sharing are reviewed. The related findings are organized and reflect the conceptual framework presented in Chapter 4.

RESPONSE RATE

Of the twenty-four Councils surveyed, seventeen coordinators remitted responses to the survey. This generated a 71% response rate. Several factors may have contributed to this relatively high response rate. Anonymity was a factor in this response rate. In addition, questions regarding the survey were directed to a member of the Texas Domestic Preparedness Program and an academic advisor who substantiated the research. This component enhanced the validity of this researched. Contacting these coordinators prior to sending the surveys also provided the respondents with feedback about the goals and objectives of this applied research project.

Here is some speculation on why surveys were not remitted. Several respondents expressed concern in answering the survey due to confidentiality factor and the sensitivity of this research. Others expressed that they did not have the knowledge or expertise on the subject matter and relayed the survey to another individual. Still others may have experienced time constraints.

Within each infrastructure, the categories within the conceptual framework and related survey questions are as follows:

- Computer System/ Cyber Vulnerabilities
- Physical Threats
- Disaster Recovery
- Information Sharing (ISAC)

Each section below outlines the findings.

I. COMPUTER SYSTEMS/CYBER VULNERABILITIES

The survey addressed key threats that impact water and electricity infrastructures such as hacking, viruses, computer worms, Trojan Horses, and denial of service attacks. These threats are highlighted in the following section and can be viewed in Tables 5.1 and 5.2. Table 5.1 reflects the response numbers for the water infrastructure and Table 5.2 reflects the response numbers for the electricity infrastructure.

A. WATER INFRASTRUCTURE

Sixty-five percent (65%) of the respondents considered computer hacking a threat to water systems (See Table 5.1). More than three-fourths (76%) of the respondents believed computer systems were vulnerable to viruses. The threat of virus findings as compared to computer worms findings are similar, with more than half of those surveyed view computer systems as vulnerable to these threats. Seven out of the ten respondents (70.1%) believed computers systems were vulnerable to computer worms. Unlike computer worms, viruses, and hacking, Trojan horses were viewed as being less of an area of concern.

The neutral response by forty-seven percent (47%) of the respondents may indicate that some respondents may not be familiar with Trojan Horses or may not view

them as much as a threat as the hacking, viruses, and computer worms. This may also indicate a false sense of security that Trojan horses are not a threat. When the vulnerability indicated denial of service attacks, nine (9) respondents agreed that computer systems that operate and/or maintain water systems were vulnerable. Thirty-five percent of the respondents were moderately concern whereas twelve percent (12%) were not concern. More than half (10) agreed that computer systems should not be accessible by remote access via modem and/or internet. The twenty-nine percent (29%) who disagreed is the highest percent number thus far in this survey. The previous numbers for a disagreed response were all twelve percent (12%) or two (2) respondents.

SUMMARY

Overall the majority of respondents agreed that hacking, viruses, computer worms and denial of service attacks are threats to computer systems that operate and/or maintain water systems. This was in agreement with most respondents indicating that remote access via modem and/or internet is not advisable; thus limiting the threats to the computer systems that can make them vulnerable. Most respondents felt neutral about the threat posed by the Trojan Horses. This may indicate that respondents are not sure what this threat represents or that infrastructures are not remotely connected to computer systems.

Computer System/Cyber Vulnerabilities-TABLE 5.1

WATER INFRASTRUCTURE N = 17		
COMPUTER SYSTEMS	**SA/A**	**Mode**
HACKING VULNERABILITY.	65%	Agree
VIRUS VULNERABILITY.	76%	Agree
COMPUTER WORM VULNERABILITY	70.1%	Agree
TROJAN HORSE VULNERABILITY.	41%	Neutral
DENIAL OF SERVICE ATTACK VULNERABILITY	53%	Agree
INACCESSIBLE BY REMOTE ACCESS	59%	Agree

B. ELECTRICITY INFRASTRUCTURE

Twelve respondents (70%) agreed, including five strongly, that computer systems which operate and/or maintain electricity are vulnerable to hacking; a 5.1% increase compared to water infrastructure (See Table 5.2). Overall seventy percent (70.1%) of these respondents (12) surveyed felt computer systems which operate and/or maintain electricity were vulnerable to viruses. Like its water infrastructure counterpart, more than half (59%) surveyed felt computer systems which operate and/or maintain electricity were vulnerable to computer worms. Six of the respondents were moderately concerned with this threat.

Once again, Trojan horses were viewed as being less of a threat. More than half (52%) of the respondents expressed neutrality when the vulnerabilities included Trojan Horses and only forty-one percent (41%) agreed that computer systems that operate and/or maintain water systems were vulnerable to Trojan Horses. When the vulnerability indicated denial of service attacks, fifty-three percent (53%) of the respondents agreed that computer systems that operate and/or maintain waters systems were vulnerable. Seven respondents were neutral with reference to this vulnerability. Sixty-five percent (65%) of the respondents agreed that computer systems should not be accessible by remote access via modem and/or internet.

SUMMARY

Overall, the majority of the respondents agreed that hacking, viruses, computer worms, and denial of service attacks are threats to computer systems that operate and/or maintain electricity infrastructures. This was in agreement with most respondents indicating that remote access via modem and/or internet is not advisable; thus limiting the threats to the computer systems that can make them vulnerable. A majority of respondents felt neutral on the Trojan Horses. The respondents were equally divided on agreeable and neutral regarding denial of service attacks. This may indicate that respondents are unsure of denial of service attack as a threat. Again, the neutral stance in regards to the Trojan Horses may demonstrate that most respondents are not aware of Trojan Horses or simply feel that electricity infrastructures are not vulnerable to this threat.

Computer System/Cyber Vulnerabilities – TABLE 5.2

ELECTRICITY INFRASTRUCTURE N = 17		
COMPUTER SYSTEMS	**SA/A**	**Mode**
HACKING VULNERABILITY.	70.1%	Agree
VIRUS VULNERABILITY.	70.1%	Agree
COMPUTER WORM VULNERABILITY	59%	Agree
TROJAN HORSE VULNERABILITY.	41%	Neutral
DENIAL OF SERVICE ATTACK VULNERABILITY	53%	Agree/ Neutral
INACCESSIBLE BY REMOTE ACCESS	65%	Agree

II. PHYSICAL THREATS

The survey addressed key threats that impact water and electricity infrastructures including destruction of systems, disruptions, fire damage, and water damage. Additional questions in the survey included reinforcements and restricting access to structures and water systems. Lastly, inquiries regarding threats to the water infrastructures that addressed chemical, radiological and biological contaminations were included. These threats are highlighted in the following section. Tables 5.3 and 5.4 highlight the response numbers for physical threats. Table 5.3 reflects the water infrastructure and Table 5.4 represents the electricity infrastructure.

A. WATER INFRASTRUCTURE

When surveyed, a vast majority (94%) agreed to reinforcing new and/or existing structures to avert physical threats on water systems (See Table 5.3). Overall, eighty-eight percent (88%) of the respondents surveyed felt there was a concern regarding this threat. However, disruption generated more of a concern with ninety-four percent (94%). A vast majority (94%) agreed that the disruption of water distribution is a concern. More than half (9) of these respondents strongly agreed that this threat was a concern.

Less than half (47%) of the respondents expressed neutrality when the vulnerabilities addressed fire damage. Over three quarters (88%) of those surveyed were concerned about power loss to the water systems. Physical threats such as destruction, disruption of water distribution, fire damage and power loss can cause alarm if they diminish the water systems. Restricting access to water systems or buildings can lower the extent of these physical threats. The next series of questions solicited some information regarding restricting access to waters systems and buildings.

All respondents (100%) yielded an agreeable response to restricting access to water systems in order to avert physical threat. Over half (10) of these were strongly agreeable to this statement. All respondents (100%) agreed that it was necessary to restrict access into buildings and computer systems to avert physical threats against water systems. Again, over half (10) were strongly agreeable to this statement. All agreed that restricting access to buildings and computer systems is necessary to avert physical threats to water systems. Even though restricting access can alleviate some concerns, water systems are vast by nature and can be accessible at numerous points. Therefore

contamination in the water systems could pose some apprehension to the public. The next series of questions dealt with chemical, radiological and biological contamination.

Overall eighty-two percent (82%) of respondents surveyed expressed concern with chemical contamination in the water systems. Unlike chemical, radiological contamination generated less favorable concern. Eleven respondents (65%) considered radiological contamination of water systems a concern. Over eighty-seven percent (87%) (15) respondents considered biological contamination of water systems a concern. Respondents were equally concerned with biological (88%) contamination and chemical contamination (88%) than radiological (65%)

SUMMARY

Overall, an overwhelming majority strongly agreed that restricting access to water systems, buildings and computer systems is necessary to avert physical threats to water systems. In essence, restricting access to targeted structures lowers the probability that physical threats will occur. In addition, the majority of the respondents agreed that reinforcement of new and existing structures is necessary to avert physical threats on water systems. In general, respondents favored reinforcement of structures and restricting access to structures to avert physical threats on water systems.

Respondents were most concerned with the disruption of water than any of the other physical threats (94%). Since water is vital to the well being of every living being, the disruption of water distribution is extremely critical. Destruction of water systems (88%) was more of a concern than power loss and fire damage. Respondents were equally concerned with power loss (88%) and destruction of a water system (88%). Fire damage was of less concern. Respondents remained neutral (41%) on this particular

threat. This may indicate that fire damage is really not an issue or considered a threat. In general, respondents were less concerned with contamination than these key threats.

Respondents were equally concerned with biological and chemical contaminations (88%). Overall, more than half respondents were concerned with contamination.

Physical Threats -TABLE 5.3

WATER INFRASTRUCTURE N = 17		
PHYSICAL THREATS	**SA/A**	**Mode**
AVERT THREATS – Reinforcement of structures	94%	Agree
DESTRUCTION.	88%	Agree
DISRUPTION	94%	Strongly Agree
FIRE DAMAGE	47%	Neutral
POWER LOSS.	88%	Agree
AVERT THREAT – Restricting access to water systems	100%	Strongly Agree
AVERT THREAT – Restricting access to buildings and computers	100%	Strongly Agree
CHEMICAL CONTAMINATION	88%	Agree
RADIOLOGICAL CONTAMINATION	65%	Agree
BIOLOGICAL CONTAMINATION	88%	Agree

B. ELECTRICITY INFRASTRUCTURE

The survey addressed key threats that impact electricity infrastructures such as destruction, disruption, fire damage, and water damage. Respondents answered inquiries related to reinforcement of new and existing structures. In addition, the survey included questions relating to restricting access to electricity supply systems, structures and computer systems within these structures. These questions revealed concerns and acknowledgment that physical threats exist.

When surveyed, a vast majority (94%) agreed to reinforcing new and/or existing structures to avert physical threats on water systems (See Table 5.4). Though each water and electricity infrastructure yielded ninety-four percent (94%) agreement, respondents here chose "strongly agreed" more often by (12%). Each of the respondents (100%) was concerned with the destruction of an electric supply system. The destruction of an electric supply would disrupt services of electricity and the distribution of drinking water.

Like destruction, all respondents (100%) were concerned with the disruption of the electricity supply system. Again, the disruption of electricity could disrupt services for the drinking water supply and extinguishing fires. Approximately eighty-eight percent (88%) of respondents surveyed indicated they were concerned with fire damage to an electricity supply system. This result may indicate that fire damage is more plausible in an electricity supply system than a water supply system. It only makes sense that fire damage could be viewed more destructive in an electricity supply system since water extinguishes fires (and electricity can cause fires).

Eleven respondents were concerned with water damage to an electrical power system. Of the four physical threats, water damage was seen as the least concern with

sixty-five percent (65%). Physical threats such as destruction, disruption of electricity supply, fire damage and water damage can cause alarm if they destroy the electricity power supply. Electrical power systems generate electricity for the water distribution system. Like the water infrastructure counterpart, restricting access to electricity supply systems or building can lower the extent of these physical threats. The next series of questions solicited some information regarding restricting access to electricity supply systems, buildings and computer systems.

A vast majority of respondents (94%) surveyed agreed that it is necessary to restrict access to electricity supply systems to avert physical threat. Only one respondent remained neutral. All seventeen respondents (100%) felt it was necessary to restricting access to buildings and computer systems to avert physical threats to the electrical grid and power supply. Nine of these respondents strongly agreed with the statement. This indicates that most if not all respondents feel it is necessary to secure the buildings and computer systems within these buildings to avert physical threats on the electrical grid and power supply.

SUMMARY

All respondents (100%) agreed that restricting access to electricity supply systems, buildings and computer systems, is necessary to avert physical threats to electrical power systems. In essences, restricting access to targeted structures lowers the probability that physical threats will occur. In addition, the majority of the respondents agreed that reinforcement of new and existing structures is necessary to avert physical threats on electricity supply systems.

Respondents were equally (100%) concerned with the destruction of electricity and the disruption of electricity supply system. The vast majority of our infrastructures rely on power proving a major concern if these systems were destroyed and/or disrupted. Some water systems are heavily reliant on electricity to provide services. Fire damage (88%) was considered more of a concern than water damage (65%). In comparing infrastructures, fire damage was more of a concern with electrical supply system (88%) than water systems (47%).

Physical Threats – TABLE 5.4

ELECTRICITY INFRASTRUCTURE N = 17		
PHYSICAL THREATS	**SA/A**	**Mode**
AVERT THREATS – Reinforcement of structures	94%	Strongly Agree/Agree
DESTRUCTION.	100%	Agree
DISRUPTION	100%	Agree
FIRE DAMAGE	88%	Agree
WATER DAMAGE	65%	Agree
AVERT THREAT – Restricting access to electricity supply systems	94%	Agree
AVERT THREAT – Restricting access to buildings and computers	100%	Strongly Agree

III. DISASTER RECOVERY

The survey addressed disaster recovery planning methods that impact water and electricity infrastructures including mirroring, hot sites, and cold sites. Additional questions in the survey included an inquiry on the on the recovery planning in local government. These recovery methods are highlighted in the following section and can be viewed in Tables 5.5 and 5.6. Table 5.5 reflects the response numbers for the water infrastructure. Table 5.6 reflects the response numbers for the electricity infrastructure.

A. WATER INFRASTRUCTURE

Three types of disaster recovery planning were examined in this section: Mirroring, hot sites, and cold sites. Respondents opined on these planning methods.

Less than half (47%) of the respondents surveyed did not agree that mirroring disaster recovery planning methods for water systems are well developed in Texas local government. One out of the eight respondents strongly disagreed. Eight respondents remained neutral on this matter.

Only twelve percent (12%) of the respondents surveyed agreed that hot site disaster recovery planning methods for water systems are well developed in Texas local government.

Respondents seem more favorable to cold site recovery planning method. Three respondents agreed that cold site disaster recovery planning methods are well developed in Texas local government. Like the other recovery methods, less than half (8) of the respondents surveyed expressed neutrality to this statement.

Less than half (8) of the respondents surveyed felt that water disaster recovery planning in Texas local government was unsatisfactory.

SUMMARY

In general, most respondents were not favorable to each recovery method. Respondents remained neutral in describing Texas local governments as well developed in all three types of planning methods Though cold sites received a favorable response with eighteen percent (18%), the overall sense was neutral. Several factors may indicate that some respondents were unfamiliar with these types of recovery planning methods or they may simply be indifferent to recovery planning methods. Still, others may not know if local governments in Texas have well developed plans in case of a disaster. In general, the respondents seemed dissatisfied with the water disaster recovery plan in Texas local government.

Disaster Recovery – TABLE 5.5

WATER INFRASTRUCTURE N = 17		
DISASTER RECOVERY	**SA/A**	**Mode**
MIRRORING	5%	Neutral
HOT SITE	12%	Neutral
COLD SITE	18%	Neutral
PLANNING IS SATISFACTORY	12%	Neutral/Disagree

B. ELECTRICITY INFRASTRUCTURE

Three types of disaster recovery planning were examined in this section: Mirroring, hot sites, and cold sites. Respondents opined on these planning methods.

Eleven respondents surveyed remained neutral regarding mirroring disaster recovery planning methods for electricity. Less than a quarter surveyed (4) disagreed with this statement. Respondents agreed more with this statement in the electricity infrastructure than in the water infrastructure.

More than half of the respondents (9) surveyed remained neutral to hot site disaster recovery planning methods for electricity. Respondents were equally divided between agreed (4) and disagreed (4). Hot site seems to be the most favorable among the three types of planning methods with (4) agreeable responses with the electricity infrastructure.

Like the mirroring planning methods, respondents remained neutral to cold site disaster recovery planning methods for electricity.

Respondents were equally divided between neutral (7) and disagreed (7) on their satisfaction level regarding electricity disaster recovery planning in Texas local government.

SUMMARY

In general, most respondents were not favorable concerning each of the disaster recovery planning methods. Overall, respondents remained neutral in describing Texas local governments as well developed in all three types of planning methods Respondents seemed more favorable to hot sites with the most agreed (4). Cold sites seem the next favorable with (3), and mirroring was the least. Several factors may indicate that some respondents were unfamiliar with these types of recovery planning methods or they may simply be indifferent to recovery planning methods. Still, others may not have direct knowledge on local governments disaster planning. In general, the respondents seemed equally dissatisfied and neutral with the electricity disaster recovery plan in Texas local government.

Disaster Recovery – TABLE 5.6

ELECTRICITY INFRASTRUCTURE N = 17		
DISASTER RECOVERY	**SA/A**	**Mode**
MIRRORING	12%	Neutral
HOT SITE	23%	Neutral
COLD SITE	18%	Neutral
PLANNING IS SATISFACTORY	18%	Neutral/Disagree

IV. INFORMATION SHARING (ISAC)

The survey addressed information sharing among local, state and federal governments. It also explored the relationship between local governments and private entities that own and/or operate water and electricity infrastructures. The responses can be viewed in Tables 5.7 and 5.8. Table 5.7 reflects the response numbers for the water infrastructure. Table 5.8 reflects the response numbers for the electricity infrastructure

A. WATER INFRASTRUCTURE

Over half (53%) of the respondents expressed dissatisfaction with sharing security measures and disaster recovery planning among local, state, and federal governments. Overall most of the respondents were not satisfied with sharing information among government entities.

More than half (53%) of the respondents were dissatisfied with information sharing between local governments and private entities that own and/or operate electricity

critical infrastructures. Overall, most respondents were not satisfied with the information sharing between government officials and private owners of critical infrastructures.

SUMMARY

The majority of the respondents felt that government officials did not share information with each other. Information such as security measures and disaster recovery planning of both electricity and water infrastructures should be discussed on a regular basis. Sharing expertise, knowledge, and methods can limit vulnerabilities and strengthen security measures that are applicable to securing public infrastructures. Sharing information is a critical factor in the Homeland Security strategy plans. Respondents may feel dissatisfied with political factors that play a role in governmental entities. Bureaucracy can prevent government agencies from executing plans.

The majority of the respondents were not satisfied with how government entities share information with private entities that own and/or operate critical infrastructures.

Information Sharing (ISAC) – TABLE 5.7

WATER INFRASTRUCTURE N = 17		
INFORMATION SHARING	**SA/A**	**Mode**
SHARING INFORMATION ALL LEVEL OF GOVERNMENTS	29%	Disagree
SHARING INFORMATION WITH PRIVATE ENTITIES	29%	Disagree

B. ELECTRICITY INFRASTRUCTURE

More than half (53%) of the respondents surveyed were dissatisfied with how information was shared among local, state, and federal government entities. These respondents do not feel that security measures and disaster recovery planning are not being shared among government officials. These respondents are Council of Government members who are intermediaries between local, state, and federal governments. Sharing information is essential for the safeguarding of infrastructures.

Less than half (47%) of the respondents surveyed were dissatisfied with how information was shared among government entities and private owners that operate and/or own critical infrastructure. These findings demonstrate that there may be minimal information sharing between private entities and governmental agencies. Again, sharing information should be vast between those who operate public infrastructures and government agencies.

SUMMARY

A majority of the respondents felt that government officials did not share information with each other. Information such as security measures and disaster recovery planning of both electricity and water infrastructures should be discussed on a regular basis. Sharing expertise, knowledge, and methods can limit vulnerabilities and strengthen security measure that is applicable to securing public infrastructures. Sharing information is a critical factor in the Homeland Security strategy plans. Respondents may feel dissatisfied with political factors that play a role in governmental entities. Bureaucracy can plague government agencies from executing plans.

The majority of the respondents were not satisfied with how government entities share information with private entities that own and/or operate critical infrastructures. Most private entities may not want to share information because proprietary information may be released to their competitors.

Information Sharing (ISAC) – TABLE 5.8

ELECTRICITY INFRASTRUCTURE N = 17		
INFORMATION SHARING	**SA/A**	**Mode**
SHARING INFORMATION ALL LEVEL OF GOVERNMENTS	29%	Disagree
SHARING INFORMATION WITH PRIVATE ENTITIES	29%	Disagree

CHAPTER SIX
CONCLUSION

INTRODUCTION

The purpose of this research is to assess the Texas water & energy infrastructures vulnerability from the point of view of Texas Regional Council leaders. The key areas of concern are physical security threats and vulnerabilities to computer systems. In addition, opinions regarding disaster recovery and information sharing are reviewed. The literature review identified some potential vulnerability of water and electricity infrastructures. A survey was developed from the conceptual framework and was sent to representatives of the twenty-four Texas Regional Councils of Government. The responses illustrated the respondents' opinions and concerns regarding the various components of computer systems and physical threats to the infrastructures. There are four tables that summarize the findings:

- Computer Vulnerability – Table 6.1
- Physical Threats – Table 6.2
- Disaster Recovery – Table 6.3
- Information Sharing – Table 6.4

Summary of Findings – Computer Vulnerability

The respondents showed a high level of concern regarding vulnerabilities on hacking, viruses, and computer worms on both water and electricity infrastructures (See Table 6.1). Most appear to be unsure about Trojan Horses. A neutral response could mean that they were unfamiliar with these types of threats. Definitions regarding the computer threats may have assisted clarifying any questions regarding these series of questions.

Respondents expressed a high level of concern for remote access to computer systems in water and electricity infrastructures. Limiting the remote access to computer systems can diminish vulnerabilities to the various threats outlined in this applied research project.

An emergency planning coordinator might disagree with this assessment, since they rely on fast actions to shut off equipment or infrastructures in order to avoid a larger catastrophe. Flooding, for instance, would require the fast action of an emergency coordinator to open storm drains remotely, rather than manually to avoid further damages.

SUMMARY OF FINDINGS –Table 6.1

Computer Vulnerability – Water	LEVEL OF CONCERN
HACKING.	HIGH
VIRUSES	HIGH
COMPUTER WORMS	HIGH
TROJAN HORSES	MODERATE
DENIAL OF SERVICE ATTACKS	HIGH
NO REMOTE ACCESS TO COMPUTER SYSTEMS	HIGH
Computer Vulnerability – Electricity	**LEVEL OF CONCERN**
HACKING	HIGH
VIRUSES	HIGH
COMPUTER WORMS	HIGH
TROJAN HORSES	MODERATE
DENIAL OF SERVICE ATTACKS	HIGH - MODERATE
NO REMOTE ACCESS TO COMPUTER SYSTEMS	HIGH

Summary of Findings – Physical Threat

Overall, the majority of respondents strongly agreed in restricting access to water systems and restricting access to structures and computer systems in both water and energy infrastructures.

The majority of the respondents felt most concern with disruption of water systems (See Table 6.2). Respondents expressed a very high level of concern over the protection of water systems in three questions out of the ten. In contrast, respondents express a very high level of concern of electricity infrastructure in only two questions out of the seven. Though most respondents reflected a high level of concern with physical threats to electricity infrastructures, respondents felt more strongly about the water infrastructures.

Overall respondents expressed a high level of concern with physical threats in both water and electricity infrastructures. The one caveat was the fire damage with relation to water systems. This particular threat was moderately received. This could mean that respondents felt that fire damage was not seen as a potential threat to water systems.

SUMMARY OF FINDINGS –Table 6.2

PHYSICAL THREAT - WATER	AVERT THREAT	LEVEL OF CONCERN
REINFORCEMENT – new and existing structures	HIGH	
DESTRUCTION		HIGH
DISRUPTION		VERY HIGH
FIRE DAMAGE		MODERATE
POWER LOSS		HIGH
RESTRICTING ACCESS – Water Systems	VERY HIGH	
RESTRICTING ACCESS – Structures and Computer Systems	VERY HIGH	
CHEMICAL CONTAMINATION		HIGH
RADIOLOGICAL CONTAMINATION		HIGH
BIOLOGOCIAL CONTAMINATION		HIGH
PHYSICAL THREAT – ELECTRICITY	**AVERT THREAT**	**LEVEL OF CONCERN**
REINFORCEMENT – new and existing structures.	VERY HIGH-HIGH	
DESTRUCTION		HIGH
DISRUPTION		HIGH
FIRE DAMAGE		HIGH
WATER DAMAGE		HIGH
RESTRICTING ACCESS – Electricity Supply Systems	HIGH	
RESTRICTING ACCESS – Structures and Computer Systems	VERY HIGH	

Summary of Findings – Disaster Recovery

The majority of the respondents were moderately satisfied with the various disaster recovery planning methods in Texas local governments (See Table 6.3). The question posed if the recovery planning methods were "well developed" in local governments. "Well developed" was not clarified in the survey. The question was not direct and may have confused respondents.

The neutral responses may indicate that respondents may not have direct knowledge with the various local governments' planning strategies. In addition, respondents may not feel comfortable remarking on this particular question.

In addition, respondents may not be knowledgeable with the concepts of mirroring, hot sites, or cold sites. Recovery methods were not defined in the survey. Definitions may have cleared up confusion on these disaster recovery methods.

A majority of the respondents were equally neutral or unsatisfied with both water and electricity recovery planning within Texas local governments. Again respondents may not be familiar with local governments' recovery planning methods, and responded in this manner.

SUMMARY OF FINDINGS –Table 6.3

WATER INFRASTRUCTURE	
DISASTER RECOVERY	**LEVEL OF SATISFACTION**
MIRRORING – Well Developed	**MODERATE**
HOT SITE – Well Developed	**MODERATE**
COLD SITE - Well Developed	**MODERATE**
PLANNING IS SATISFACTORY	**MODERATE - LOW**

ELECTRICITY INFRASTRUCTURE	
DISASTER RECOVERY	**LEVEL OF SATISFACTION**
MIRRORING	**MODERATE**
HOT SITE	**MODERATE**
COLD SITE	**MODERATE**
PLANNING IS SATISFACTORY	**MODERATE-LOW**

Summary of Findings – Information Sharing

The majority of the respondents expressed dissatisfaction with information sharing among government officials in both water and electricity infrastructures (See Table 6.4). They also were dissatisfied with information sharing between local government officials and private entities in both water and electricity infrastructures. Information sharing could be limited by political interest and/or bureaucracy. In addition, information sharing with private entities may pose problems with trust. Private entities have the most to lose if their proprietary information is released to their competitors.

Texas has initiated steps to protect documents from being released under the Homeland Security Bill, House Bill 9 which was passed in May 2003 (Wade, 2003, page 24). This bill provides an exemption for documents that would reflect vulnerability assessments or homeland security components. Given this tool, private entities may be proactive in sharing information with government entities. As was mentioned in literature review, most private entities have Information Sharing and Analysis Center (ISAC) communities. Local governments benefit if they took a proactive role in creating an ISAC partnerships within the community.

SUMMARY OF FINDINGS –Table 6.4

WATER INFRASTRUCTURE	
INFORMATION SHARING	**LEVEL OF SATISFACTION**
SHARING INFORMATION ALL LEVEL OF GOVERNMENTS	**LOW**
SHARING INFORMATION WITH PRIVATE ENTITIES	**LOW**
ELECTRICITY INFRASTRUCTURE	
INFORMATION SHARING	**LEVEL OF SATISFACTION**
SHARING INFORMATION ALL LEVEL OF GOVERNMENTS	**LOW**
SHARING INFORMATION WITH PRIVATE ENTITIES	**LOW**

Suggestions for Future Research

The purpose of this research is to assess the Texas water & energy infrastructures vulnerability from the view point of Texas Regional Council leaders. The key areas of concern are physical security threats and vulnerabilities to computer systems. In addition, opinions regarding disaster recovery and information sharing are reviewed

Due to the nature of this applied research study, most respondents were apprehensive about providing confidential information. Research information on vulnerabilities assessment are regarded confidential and posed problems in obtaining data. To secure valuable information regarding this matter, one would need to assure these respondents that their perceptions and opinions would remain confidential and is part of a valid research project.

Future research studies can include the preparedness levels of the counties or cities. Research of this type would provide a more direct approach in obtaining opinions in local governments. Mayors and county commissioners can espouse their opinions on the subject matter.

This applied research project did not address remediation plans, if there were any, concerns on the physical threats, and computer vulnerabilities of water and energy infrastructures. A series of questions on how one would fix these vulnerabilities could have been addressed.

In addition, computer vulnerabilities and information technology were viewed important in this applied research project. Information technology experts should collaborate with governments and private entities to ensure security measures and policies are implemented for computer systems that communicate with water and energy

infrastructures. Moreover, private entities operating these infrastructures should collaborate with governments to ensure that these computer systems are safeguarded from physical and cyber threats. ISAC can be created through this partnership. Future research projects could examine ISAC within Texas communities.

Throughout this research project, literature addressed identification of the critical infrastructure and the identification of the vulnerabilities to these infrastructures. Future research studies could address these vulnerabilities and ask respondents if they conduct periodical testing for new threats.

This applied research project did not focus on funding for vulnerabilities assessments and proactive measures. Future research projects could provide assessments on how local governments obtain funding from federal and state resources. Local governments need these resources to address the growing budget that have left many strapped for monies. A practical ideal type could provide a checklist on the methods in obtaining funding for Homeland Security initiatives.

This study illustrates the concerns of these respondents who represent part of the Texas Homeland Security initiatives. These concerns echo the anxiety that most feel around the country. Security means safety. Citizens want accountability and would like to feel safe from terrorist acts. At this time, most terrorists are developing ways to exploit information and plan out innovative and disastrous attacks. Americans want to feel safe in their communities. They look upon their government officials to provide this security for them.

APPENDIX A

APPENDIX B

Attached for your review is a survey that we discussed regarding Texas Regional Councils of Governments' assessment of water and electricity vulnerabilities in Texas. This survey is part of an applied research project pursuant to a Masters in Public Administration at Texas State University at San Marcos, Tx.

Please take a few minutes to fill this survey out and provide your assessments regarding water and electricity in Texas. I would like to assure you that individual responses will not be identified or published in my report due to nature of this subject matter. I will be generating statistical analysis base from responses generated for this applied research project.

Please send your completed survey as soon as possible to one of the following addresses:

Lcantu3@austin.rr.com
Or 3400 Dunliegh, Austin, TX 78745

A timely response is deeply appreciated.

You can verify the validity of my applied research project by contacting either my academic advisor and/or Barry Good at:

Dr. Patricia Shields
Texas State University
(512) 245-2143
ps07@txstate.edu.

Barry Good
Texas Engineering Extension Service
(970) 458-6943
james.good@@teexmail.tamu.edu

If you have any questions or comments, please contact me at 293-2680 or via e-mail.

If you are interested in receiving the results of this survey, I will gladly furnish them to you at your request. Thank you for your assistance and participation.

Sincerely,

Lucinda Cantu
Graduate Student
Texas State University at San Marcos

APPENDIX B -1

This is a friendly reminder regarding the survey that I sent to you last week. I am under some time constraints regarding the responses on this survey. I will be needing a response to this survey by Saturday, March 20, 2004 in order to do the analysis for my applied research project. Any input is greatly appreciated. Below is information regarding this survey.
Thank you - Lucy Cantu
****
Attached for your review is a survey that we discussed regarding Texas Regional Councils of Governments' assessment of water and electricity vulnerabilities in Texas. This survey is part of an applied research project pursuant to a Masters in Public Administration at Texas State University at San Marcos, Tx.

Please take a few minutes to fill this survey out and provide your assessments regarding water and electricity in Texas. I would like to assure you that individual responses will not be identified or published in my report due to nature of this subject matter. I will be generating statistical analysis base from responses generated for this applied research project.

Please send your completed survey as soon as possible to one of the following addresses:

Lcantu3@austin.rr.com
Or 3400 Dunliegh, Austin, TX 78745

A timely response is deeply appreciated.

You can verify the validity of my applied research project by contacting either my academic advisor and/or Barry Good at:

Dr. Patricia Shields
Texas State University
(512) 245-2143
ps07@txstate.edu.

Barry Good
Texas Engineering Extension Service
(970) 458-6943
james.good@@teexmail.tamu.edu

If you have any questions or comments, please contact me at 293-2680 or via e-mail.

If you are interested in receiving the results of this survey, I will gladly furnish them to you at your request. Thank you for your assistance and participation.

Sincerely,

Lucinda Cantu
Graduate Student
Texas State University at San Marcos

APPENDIX C

Please indicate how strongly you agree or disagree with the following statements with regards to the following questions:

SA –	**Strongly Agree**	**N -**	**Neutral**
A -	**Agree**	**D -**	**Disagree**
N -	**Neutral**	**SD-**	**Strongly Disagree**

Critical Infrastructure: Water

These questions relate to computer systems that operate and maintain the water sources and/or systems in Texas:

1. Computer systems that operate and/or maintain water systems are vulnerable to hacking.	SA	A	N	D	SD
2. Computer systems that operate and/or maintain water systems are vulnerable to viruses.	SA	A	N	D	SD
3. Computer systems that operate and/or maintain water systems are vulnerable to computer worms.	SA	A	N	D	SD
4. Computer systems that operate and/or maintain water systems are vulnerable to Trojan Horses.	SA	A	N	D	SD
5. Computers systems that operate and/or maintain water systems are vulnerable to denial of service attacks.	SA	A	N	D	SD
6. Computer systems that operate and/or maintain water systems should not be accessible by remote access via modem and/or internet.	SA	A	N	D	SD

These questions relate to Physical Threats on critical infrastructure of **water sources in Texas:**

7. Reinforcement of new and/or existing structures is necessary to avert physical threats on water systems.	SA	A	N	D	SD
8. Destruction of water systems is a concern.	SA	A	N	D	SD
9. Disruption of water distribution is a concern.	SA	A	N	D	SD
10. Fire damage to water systems is a concern	SA	A	N	D	SD
11. Power loss to water systems is a concern.	SA	A	N	D	SD
12. Restricting access to water systems are necessary to avert physical threat	SA	A	N	D	SD
13. Restricting access to buildings and computer systems are necessary to avert physical threats to water systems.	SA	A	N	D	SD
14. Chemical contamination of water systems is a concern.	SA	A	N	D	SD
15. Radiological contamination of water systems is a concern.	SA	A	N	D	SD
16. Biological contamination of water systems is a concern.	SA	A	N	D	SD

Critical Infrastructure: Energy

These questions relate to computer systems that operate and maintain the electrical grid and electricity supply systems in Texas:

17. Computer systems that operate and/or maintain electricity are vulnerable to hacking.	SA	A	N	D	SD
18. Computer systems that operate and/or maintain electricity are vulnerable to viruses.	SA	A	N	D	SD
19. Computer systems that operate and/or maintain electricity are vulnerable to computer worms.	SA	A	N	D	SD
20. Computer systems that operate and/or maintain electricity are vulnerable to Trojan Horses.	SA	A	N	D	SD
21. Computers systems that operate and/or maintain electricity are vulnerable to denial of service attacks.	SA	A	N	D	SD
22. Computer systems that operate and/or maintain electricity should not be accessible by remote access via modem and/or internet.	SA	A	N	D	SD

These questions relate to Physical Threats on electrical grid and power supply systems in Texas:

23. Reinforcement of new and/or existing structures is necessary to avert physical threats on electricity supply system.	SA	A	N	D	SD
24. Destruction of electric supply system is a concern.	SA	A	N	D	SD
25. Disruption of electricity supply system is a concern.	SA	A	N	D	SD
26. Fire damage to electricity supply system is a concern.	SA	A	N	D	SD
27. Water damage to electricity power system is a concern.	SA	A	N	D	SD
28. Restricting access to electricity supply systems is necessary to avert physical threat.	SA	A	N	D	SD
29. Restricting access to buildings and computer systems is necessary to avert physical threats to electrical grid and power supply.	SA	A	N	D	SD

DISASTER RECOVERY/INFORMATION SHARING (ISAC)

WATER INFRASTRUCTURES					
30. Mirroring disaster recovery planning methods for water are well developed in Texas local government.	SA	A	N	D	SD
31. Hot site disaster recovery planning methods for water are well developed in Texas local government.	SA	A	N	D	SD
32. Cold site disaster recovery planning methods for water are well developed in Texas local governments.	SA	A	N	D	SD
33. Water disaster recovery planning in Texas local government is satisfactory.	SA	A	N	D	SD
34. Sharing information regarding security measures and disaster recovery planning of water infrastructures among local, state and federal government entities is satisfactory.	SA	A	N	D	SD
35. Texas local governments and private entities that own and/or operate water critical infrastructures share information regarding security measures and disaster recovery planning on a satisfactory level.	SA	A	N	D	SD
ELECTRICITY INFRASTRUCTURES					
36. Mirroring disaster recovery planning methods for electricity are well developed in Texas local government.	SA	A	N	D	SD
37. Hot site disaster recovery planning methods for electricity are well developed in Texas local government.	SA	A	N	D	SD
38. Cold site disaster recovery planning methods for electricity are well developed in Texas local governments.	SA	A	N	D	SD
39. Electricity disaster recovery planning in Texas local government is satisfactory.	SA	A	N	D	SD
40. Sharing information regarding security measures and disaster recovery planning of electricity infrastructures among local, state, and federal government entities is satisfactory.	SA	A	N	D	SD
41. Texas local governments and private entities that own and/or operate electricity critical infrastructures share information regarding security measures and disaster recovery planning on a satisfactory level.	SA	A	N	D	SD

Bibliography

2001 Annual Report, Texas Natural Resource Conservation Commission

Allen, Tom. "Twelve Steps to Assessing Vulnerability." *Government Security*, February 2003. Page 8.

Anderson, Teresa. "A Year of Reassessment" *Security Management*. January 2003, page 61-65

Associated Press. "Key Internet servers hit by attack." CNN.com/Technology http://www.conn.com2002/TECH/internet/10/23/internet.attaack.ap/ October 23, 2002

Austin American Statesman, Business Digest, February 2004

Babbie, E. "*The Practice of Social Research, 9th Edition*", Belmont CA: Wadsworth Publishing/Thompson Learning, Inc.

Bennett, Senator Robert F. "Security in the Information Age: We're Not In Kansas Anymore" Security in the Information Age; New Challenges, New Strategies: Joint Economic Committee, United States Congress, May 2002,

CACI International, Inc. website "Computer Security Threat Table", February 2004. <http://www.caci.com/business/ia/threats.html>

Cities United for Science Progress (CUSP), "HOMELAND SECURITY: MAYORS ON THE FRONTLINE; Executive Summery of Findings", Emergency Preparedness Survey, Partnership of US Conference of Mayors and DuPont, 2002

Chiruvolu, Ravi. "Drilling Down Against Terrorism." Venture Capital Journal. April 1, 2003.

Davies, Thomas R. "EYE ON THE STATES: States Slow to Prepare IT Infrastructure for Future Attacks", *Washington Technology*, Vol.16., No. 17, November 19, 2001

Denning, Dorothy, "Cyberterrorism", Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services, U.S. House of Representatives, May 23, 2000.

Devost, Matthew G. and Perry, Steven "Ready The Defense", *Government Technology*, Volume 25, Issue 3, February 2002

EROT, Electric Reliability Council of Texas, Inc, http.www.ercot.com, 2004

Gelinas, Ulric J. and Steve G Suttton. *Accounting Information Systems. 5th Edition*, Southwestern 2002.

Hanning, Scott. "Recovering from Disaster: Implementing Disaster Recovery Plans Following Terrorism" SANS Institute, September 21, 2001 <http://www.sans.org/rr/recovery/terrorism.php>

Harowitz, Sherry L. "The New Centurions." Security Management. January 2003, Pages 51-58

Harris, Blake and Borchgrave, Arnaud de, "The Next Generation of Terrorism", Government Technology, Volume 25, Issue 3, February 2002

Haurwitz, Ralph K.M., "Hacker steal vital data about UT students, staff", Austin American Statesman, March 6, 2003.

Hulme, George, "Rising Threat – As war looms, the risk of cyberattacks form hackers and terrorists grows Are you ready?", InformationWeek, March 10, 2003

IBM UPS System website http://www.reliableups.com, April 2004

Juster, Keenneth I. and John S. Tritak, "Critical Infrastructure Assurance: A conceptual Overview"Security in the Information Age; New Challenges, New Strategies" Joint Economic Committee, United States Congress, May 2002

Krazit, Tom. "IT pros foresee major cyberattacks on horizon" Network World Fusion July 24, 2002, http://www.nwfusion.com/news/2002/0724secure.html

Krebs, Brian. "Hackers Embrace P2P Concept: Experts Fear 'Phatbot' Trojan Could Lead to New Wave of Spam or Denial of Service Attacks", Washington Post, http://www.washingtonpost.com, March 17, 2004

Krupa, Andy. "The Oversight of Physical Security and Contingency Planning" SANS Institute August 21, 2001, <http://www.sans.org/rr/recovery/oversight.php>

Lam, Beekey, and Kevin Cayo, "Can you Hack It?, Security Management, February 2003.

Laudon, Kenneth and Jane P. Laudon, "*Management Information Systems: Managing the Digital Firm*" 7th Edition, Prentice Hall, 2002

National Infrastructure Protection Center, Cybernotes, Issue #2002-23, November 18, 2002

National White Collar Crime Center (NWCCC), "'True' Computer Crime", WCC Issue, September 2003

Pangi, Robyn. "After the Attack: The Psychological Consequences of Terrorism." Perspectives on Preparedness. No. 7, John F. Kennedy School of Government, Harvard University, August 2002

Security Management. "Employee Monitoring: News and Trends." January 2003, Page 25.

Shields, P. "Pragmatism as Philosophy of Science: A Tool for Public Administration. Research in the Public Administration", 4, 199-230, 1998

Texas Association of Regional Councils, February 2004, http: wwwtxregionalcouncil.org/

Texas Department of Health, < **http://tdh.state.tx.us**>, April 2004

Texas State Data Center, (Appendix A), Texas State Data Center, February 2004, <http://txsdc.utsa.edu/maps/reference/tx_cog.pdf>

Texas Homeland Security Strategic Plan, January 30, 2004: **http://www.governor.state.tx.us/divisions/press/pressreleases/files/thsplan.pdf**

Texas Public Utility Commission (TPUC) "Self Evaluation Report to Sunset Commission", August 2003

Thibodeau, Patrick. "Terrorism fight could prompt new cyberattacks." Computerworld, http://www.computerworld.com/securitytopics/security/story/0,10801,64255,00.html Sepptember 26, 2001

Turban, McLean, and James Wetherbe, *Information Technology for Management: Tranforming Business in the Digital Economy, 3rd Edition*, John Wiley & Sons, Inc., 2002

United States Department of Homeland Security (US DHS) website, http://www.dhs.gov/ April 2004

United States Department of Homeland Security (US DHS, Ready.gov) website, http://www.ready.gov/(radiation, chemical, biological).html

United States General Accounting Office (GAO), "Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism'. GAO-04-408T, February 3, 2004

United States General Accounting Office (GAO), "Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sector". GAO-03-233, February 2003

United States General Accounting Office (GAO), "Drinking Water: Experts'Views on How Future Federal Funding Can Best Be Spent to Improve Security", GAO-04-29, October 2003

Virus or Hoax?, http://www.virusall.com/index.html, April 2004

Wade, Beth. "Security Through Secrecy", Government Security, November 2003

Weaver, Paxson, Staniford, Robert Cunningham, "A Taxonomy of Computer Worms" Defense Advanced Research Projects Agency, contract N66001-00-C-8045, October 27, 2003

Whitehouse.gov "The National Strategy to Secure Cyberspace", February 2003 http://www.whitehouse.gov/pcipb/

Whitehouse.gov, "The National Strategy to Secure Cyberspace, President's Critical Infrastructure Protection Board" <hhtp://www.whitehouse.gov/picpb/cyberstrategy-draft.html

Whitehouse.gov, "The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (Strategy)", February 2003, http://www.whitehouse.gov/pcipb/physical.html

White Paper – the Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63 (PPD 63), May 22, 1998

Zetter, Kim, "DEF CON: Trojan horse technology exploits IE hole", PC World.com, Network World Fusion, www.nwfusion.com/news/2002/0806trojan.html, August 6, 2002