Abstract

The electric grid is one of eighteen critical infrastructures in the United States that is at risk from cyber attacks. As critical infrastructures become more reliant on networked systems, it is likely that the threat of cyber attacks will increase. These types of attacks are easily executed, inexpensive, and may be performed from anywhere in the world, making it an all too popular tool among hackers and terrorists.

Cyber attacks launched against the electric grid have serious economic impact. The banking and financial sectors rely heavily on electricity to facilitate transactions via computer networks. Due to increased reliance on electricity, it is important that both physical security and cyber security of the electric grid is improved.

The United States and Australia have established and implemented critical infrastructure protection strategies to protect against cyber based threats. This research established that there is a need for the public and private sectors to partner in regard to critical infrastructure cyber security, specifically the electrical grid. The ability of a nation to adequately defend against cyber attacks is highly dependent upon information sharing between private industry and government.

Research concluded that the United States information protection regulations are stronger than Australia's. The Australian government has a laissez faire approach to information protection as opposed to a highly enforced compliancy standard, as implemented in the United States. Further research into how other countries are regulating cyber security is required to provide insight into an effective information protection strategy for the future of critical infrastructures.

THE CURRENT STATE OF CRITICAL INFRASTRUCTURE PROTECTION: THE UNITED STATES ELECTRIC GRID

by

Jessica Katz

A Research Project Submitted to the Faculty of

Utica College

December, 2011

In Partial Fulfillment of the Requirements for the Degree

Master of Science

Table of Contents

List of Illustrative Materials

Acknowledgement

First I would like to thank my husband, Dave, for his support, encouragement and patience throughout this graduate program. I would also like to thank my family, friends and Cohort 21 classmates for all the support they showed these last few years. Lastly, I would like to thank my research committee Professor Chris Riddell, Norman Good, and Daniel Didier for their guidance and assistance during the development of this paper.

The Current State of Critical Infrastructure Protection: the United States Electric Grid

The United States (U.S.) electric grid is at risk from network attacks compromising the system and leaving Americans in the dark. Computer systems networked together "form the nerve center of the country's critical infrastructure" (Condron, 2007, p. 407), and intelligence officials have stated that they are worried about cyber attackers taking control of electrical facilities via the Internet. In 2009, cyber spies from Russia and China allegedly broke into the U.S. electrical grid, leaving behind software programs that could later be used to disrupt the system (Gorman, 2009).

The federal government has determined that the energy sector is one of the eighteen critical infrastructures in the United States. Critical infrastructure is defined by federal law as the "assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof" (Department of Homeland Security [DHS], 2010, para. 2).

As critical infrastructures become more heavily supported by networked systems, it is likely that cyber attacks will increase. "Security experts predict that cyberattacks against critical infrastructures will increase as these systems increasingly move towards digitization and cybercriminals become more sophisticated" (Rege-Patwardhan, 2009, p. 265). A study conducted in 2010 on behalf of McAfee and the Center for Strategic and International Studies, showed that 80% of critical infrastructure companies faced a large-scale denial of service attack, and almost 40% of respondents detected them monthly (Hoover, 2011). In 2009 almost half of all companies surveyed experienced no denial of

service attacks whatsoever. Based on this information, and the ever increasing number of cyber assets, attacks against these systems are likely to increase. Cyber attacks are easy and inexpensive attacks that can be performed from anywhere in the world. Anonymity of an attack makes it a popular choice among hackers and terrorists.

The purpose of this study was to explore the cyber based threats associated with the U.S. electric grid and the programs in place to protect against them. Research into the methods of past attacks will help to identify where networks and computer systems may be strengthened. The cyber health of the U.S. and Australia will be analyzed to reveal how both countries protect their infrastructures. This research will explore if there is a need for the public and private sectors to form a partnership in regard to the cyber security of critical infrastructure; specifically the electrical grid. The research will also explore whether or not financial institutions have adequate safeguards in place for backup operations and if the financial industry could survive a catastrophic cyber security attack against the electric grid.

The selection of the U.S. and Australia was based on the fact that Australia is voluntary in terms of regulation for critical infrastructure protection, whereas the U.S. has moved towards mandatory regulation in the energy sector. This is evidenced with President Barack Obama's Cyberspace Policy Review in 2009. “The model adopted in Australia is very similar to the US model and relies on voluntary, industry self-regulation with little government intervention” (Corones & Lane, 2010, p. 15). The model requires active participation by owners and operators of critical infrastructure in Australia.

Research of the U.S. electric grid will be limited in scope to the northeastern region. The North American Electric Reliability Corporation’s (NERC) Critical

Infrastructure Program coordinates efforts to improve physical security and cyber security for the bulk power system of North America. These efforts include standards development, compliance enforcement, assessments of risk and preparedness, disseminating critical information via alerts to the industry, and raising awareness of key issues.

The Northeast Power Coordinating Council (NPCC) carries out the compliance enforcement for the NERC. The NPCC's geographic area includes New York and the six New England states. The organization works to enhance the reliability of the international, interconnected bulk power system in Northeastern North America through the development of regional reliability standards, coordination of system planning, design and operations, assessment of reliability, and compliance assessment and enforcement of reliability standards.

Cyber attacks against the electric grid have potential economic costs associated with them because most businesses cannot operate without electricity. The Electricity Consumers Resource Council (ELCON) summarized the costs associated with a blackout in 2003. The study by CrainTech, Case Western Reserve University's Center for Regional Economic Issues and Mirifex System LLC, produced the following findings based on a survey of businesses in Ohio, New York, Pennsylvania, Michigan, Wisconsin, and Southern Canada:

- A quarter of the businesses surveyed (24%) lost more than $50,000 per hour of downtime (*i.e.,* $400,000 for an 8-hour day), and 4% of the businesses lost more than $1 million for each hour of downtime.

- Almost 11% of firms said the blackout would affect their decision-making with regards to either growth at the current location or relocation.

Given these statistics and the fact that business such as the stock markets, airports, and banks all rely on electricity to operate, the U.S. economy would be crippled without the major power grids functioning. The banking and financial sectors specifically would be greatly disrupted and would suffer economic damage with the loss of electric power. This sector of the U.S. economy relies heavily on electric power to facilitate its transactions via computer networks. Due to increased reliance on the electric system, it is important that both the physical security and cyber security for the electric grid is improved.

Because more than 80% of U.S. energy is generated by private companies, it is important for industry best practices to be implemented and enforced. There must be a partnership between public and private sectors to ward off dangerous threats to critical systems and information technology (IT) infrastructure. To facilitate this partnership, additional information sharing must take place between the parties. Gerry Cauley, president and CEO of the NERC, said in testimony before the House Committee on Homeland Security in 2011, that a lack of real-time, actionable intelligence sharing on attacks leaves the power industry at best a step behind the government in preventing attacks.

As cyber threats and vulnerabilities for critical infrastructure continue to rise, Hoover (2011) notes that more than 40% of U.S. based critical infrastructure companies still have no interaction with the federal government on cyber defense matters, according to a survey of more than 200 critical infrastructure executives. The U.S. government falls

behind other countries in working closely with private industry on cyber security issues. For example, only about 5% of Chinese executives said that they had not worked with their government on network security, as compared to 40% of executives in the U.S.

Information sharing among private companies and government is important, but it is not enough. Private companies also need to pay more attention to defending against attacks and developing real-time identification and responses as they occur. To be truly effective in combating these attacks, companies need to move their security practices from a reactionary position to a more proactive and preemptive one. Organizations like NERC are positioning energy companies to do just that. The Critical Infrastructure Protection (CIP) reliability standard addresses the areas of security controls, training, incident response and planning, and asset recovery plans.

Literature Review

Experts believe that most of the systems supporting the nation's critical infrastructure were not designed with cyber security in mind (Baker, Filipiak, & Timlin, 2011). The primary concern within the electric sector has always been maintaining an efficient system and a steady supply of power for users. "Even today, many electric companies still use vendor default passwords because they allow easy access in times of crisis or for maintenance and repair" (Baker et al., 2011, p. 8). Ease of use does not always go hand in hand with security, but security needs to come first, especially as the number of attacks continues to increase.

Recent efforts to modernize the systems supporting the power grid have increased its efficiency but have also created new security holes which need to be addressed. The consequences associated with these security holes was demonstrated during tests

conducted at Idaho National Labs in 2007. Lewis (2010) discussed how researchers proved that by gaining remote access to the control systems of a generator and remotely changing its operating cycle, they could send it out of control. A video of the incident shows the generator shaking, smoking, and grinding to a stop. These diesel-electric generators are expensive, costing about $1 million and can take weeks or months to repair or replace, potentially leaving businesses and Americans without power for a substantial amount of time.

Many major world powers have the capability to mount a cyber attack against critical infrastructure (Baker et al., 2011). President Obama (2009) stated in a speech that:

> Cyber security is a matter of public safety and national security. We count on computer networks to deliver our oil and gas, our power and our water. We rely on them for public transportation and air traffic control. Yet we know that intruders have probed our electrical grid and that, in other countries, cyber attacks have plunged entire cities into darkness… Indeed, in today's world, acts of terror could come not only from a few extremists in suicide vests but from a few keystrokes on the computer – a weapon of mass disruption. (para. 14)

Both the economy and the national security of the U.S. have become dependent on the Internet. As long as the Internet remains vulnerable to malicious code and profitable opportunities exist for cyber criminals, then it is very likely that cyber crime will continue to affect critical infrastructure. It is imperative that countries invest in the resources necessary to increase the security of the computer systems that form the backbone of critical infrastructures. Doing so will require cooperation and resources from both government and private industry. Hoar (2005) echoed this point when he said "Our

economy and national security are dependent upon the Internet, and will continue to be adversely impacted by cybercrime" (p. 13).

The federal government has identified eighteen critical infrastructures in the U.S.: agriculture and food; banking and finance; chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; government facilities; healthcare and public health; information technology; national monuments and icons; nuclear reactors, materials and waste; postal and shipping; transportation systems; and water. These critical infrastructures are vital to the U.S., so much so, that if they become incapacitated in any way it would have a devastating impact on the economy. Each of these infrastructures is highly interconnected and in many cases, a failure in one will result in a failure of another. For example, an electrical blackout in 2003 affecting millions of people "meant more than the loss of lights or air conditioning: the critical infrastructures of transportation, emergency services, information and telecommunications, and even food, began to fail" (Whitley, Koenig, & Roberts, 2007, p. 269).

Over the years, members of Congress have conveyed concerns that hackers or terrorists will attack our nation's critical infrastructure via by exploiting cyber security weaknesses. The House Committee on Science held hearings in 2005 on the vulnerabilities associated with the nation's critical infrastructure. Committee chairman, Sherwood Boehlert, opened the hearing by stating that the U.S. is inadequately prepared to prevent, detect, and respond to cyber attacks. Chief information officers of major critical infrastructure owners and operators have also warned "that the nation's critical

infrastructure remains vulnerable to cyber attack [and] . . . that a major attack could result in significant economic disruption and loss of life" (Whitley et al., 2007, p. 271).

Vulnerabilities

As time progresses, critical infrastructures and key cyber assets have become network-centric. The prevalent use of "Supervisory Control and Data Acquisition (SCADA) systems have led to cyberdependent systems that were designed and implemented in an era when network trespass and manipulation were not relevant as these systems were not connected to the Internet" (Rege-Patwardhan, 2009, p. 261). In the electric sector, SCADA systems monitor and control the infrastructure. SCADA networks consist of a set devices such as controllers, sensors, actuators, and communication devices that are networked together. Attackers perform reconnaissance, or information gathering, on portions of these networks via the Internet giving them the ability to attack critical infrastructures from anywhere in the world with just a keyboard and a mouse.

Prior to the modernization of networks, SCADA systems operated in isolated environments where they rarely shared information with systems outside their domains. Over time, many of these systems have become interconnected to the outside world using Internet-based standards and protocols. Couple this with the fact that these control networks have become incorporated into larger corporate networks to facilitate the sharing of valuable data and the probability of a cyber attack has increased substantially.

Overall, most security vulnerabilities in critical infrastructure include failures to adequately define sensitivity levels for data, identify and protect a security perimeter, and implement access restriction based on necessity and operational requirements. Many of

these issues result from a lack of "security governance and administration, as well as budgetary pressure and employee attrition in system automation" (DePoy, Dillinger, Stamp, & Young, 2003, p. i). System administrators also create vulnerabilities because of a lack of adequate training and education.

An essential characteristic of secure information systems is the identification and classification of data into categories of similar sensitivity. Absence of these fundamental distinctions makes it impractical and futile to identify where security precautions, such as which communication link to secure and which databases require protection are appropriate. In many cases, a lack of data classification is a direct result of inadequate administration in critical infrastructure security.

Security policies help to alleviate the problems that may be caused by uneducated and unguided system administrators. Security policies define a framework for administrators to follow and are designed to help improve security and reduce the threat of cyber attacks. Historically, few critical infrastructures were managed by security policies. "Systems without security policy and administration do not possess measurable, self-perpetuating security, and experience has shown that each ungoverned information network will eventually sprout vulnerabilities" (DePoy et al., 2003, p.7). Policy is the foundation for secure system implementation, operation, and maintenance. Procedures that contribute to security are derived from elements of a security policy. Important components of security procedures are security plans, implementation guides, and security enforcement including auditing controls and sanctions.

Methods of Attacks

The most common method for a cyber attack is searching for vulnerable infrastructure software, which is often readily accessible and easy to compromise (Rege-Patwardhan, 2009). Examples would be bugs or loopholes in infrastructure software, which allow access without having to modify the system. After gaining access, attackers have the ability to attack operating systems, networks, databases, and other system applications to manipulate the behavior of infrastructure systems. One example occurred when "SCADA systems used by the Australian sewage pumping station and the US electrical grids were easily accessible on the Internet and used default passwords, which made them vulnerable to hack-attacks" (Rege-Patwardhan, 2009, p. 267).

Rootkits. Rootkits are commonly used by hackers to conduct cyber attacks. A rootkit is a piece of software that can be installed and hidden on a computer without the owner's knowledge (US-CERT, 2006). Rootkits are typically included in a larger software package or installed by an attacker that either convinced the operator to unknowingly download it or took advantage of vulnerabilities on the computer. Rootkits have malicious services running that "allow undetected operation while stealing information, monitoring user actions, modifying programs, or changing security settings to enable remote control. Some rootkits have very sophisticated capabilities, such as encrypted communications sent to a master controller that installs malware updates" (McAfee, 2010, p. 5).

Typically, an attacker installs a rootkit on a computer after obtaining root-level access, either by exploiting a known vulnerability or by obtaining a password through cracking the encryption or social engineering. Once a rootkit is installed, it allows an

attacker to conceal the ongoing intrusion and maintain privileged access to the computer by avoiding normal authentication and authorization procedures. Detection for rootkits is difficult because many times the malware is able to elude software that is intended to detect it, making removal complicated or nearly impossible.

Viruses. Viruses are the original form of malware. A virus is a program that replicates itself and tries to alter the behavior of the computer without the user's permission. Rather than targeting a software vulnerability or security hole, viruses contain software that infects other programs. To propagate the virus, a user must open a link or execute the program. “Viruses originally spread from infected data on magnetic disks or tapes to computers. Networks have accelerated a virus’s ability to spread and have magnified their impact” (McAfee, 2010, p. 6).

A virus will attempt to overwrite data, change the way another program operates, or damage the computer by altering key operating system files. Some viruses even infect files without increasing their sizes or damaging files by overwriting unused areas of the executable. Viruses try to avoid detection by killing the tasks associated with antivirus software before the software can detect the viruses. Some viruses can be safely removed by anti-virus software and others are so destructive that a reinstallation of damaged programs or the operating system is necessary. Anti-virus software must be frequently updated to keep up with the new versions of viruses that are created on a regular basis, making viruses an ongoing issue for users.

Worms. Worms target computers rather than executable software programs. A worm is able to self-propagate by making a copy of itself from one computer to another (McAfee, 2010). They typically lack the sophisticated logic found in viruses and may

cause damage by consuming bandwidth and overloading computers or networks. In today's environment, most worms attempt to spread through email (Minatel, 2011).

Some worms are designed to do more than just spread; they have payload code built in that delete files on a computer system, encrypt files in an attack, or send documents via email. One of the most common payloads is to install a backdoor in the infected computer to allow the computer to be controlled remotely. Networks of these compromised systems are then used to send out spam, attack networks and perform other malicious activities. Worm writers have been caught selling lists of IP addresses for compromised systems and others have attempted to blackmail companies by threatening a large scale attack.

As is the case with viruses, anti-virus software coupled with anti-spyware software can be helpful in worm removal. However, these programs need to be kept up to date and cannot always detect new code. Firewalls are recommended to help block worms and to prevent infected systems from infecting systems on external networks.

Trojans. Trojans pretend to be something they aren't. They appear harmless but conceal the most frequently used malware, allowing an attacker to have remote access to a system and the ability to perform various operations. Trojans are usually distributed by infected programs, which is the main reason why computer users are warned to not open any attachments or files received from untrusted sources. Trojans may also be installed from malicious websites without the user knowing in what is called a drive-by download. “Simpler Trojan horses just claim to be one thing (a picture viewer for example) when they are actually another (code that will overwrite your boot sector for example)” (Minatel, 2011, para. 6).

Botnets. Botnets are a collection of compromised computer systems connected to the Internet (McAfee, 2010). Each system in the collection is called a bot (short for robot) and is used for malicious purposes. When a computer is compromised, it becomes a part of a botnet and is controlled by an outside source typically via network protocols. An attacker usually gains control of the bots by infecting them with a virus or other malicious code that gives the attacker access. Botnets often go undetected with end users believing that their system is operating normally. Botnets are often used to perform a range of activities, from spreading spam and viruses to conducting denial-of-service attacks.

Distributed denial of service attacks. One of the most prevalent forms of cyber attacks is a distributed denial-of-service attack (DDoS). DDoS attacks are the most potent form of cyber attack because they jam servers and network infrastructure in a way that is hard to stop and may prevent companies and users from conducting day-to-day business. A DDoS attack is when a large number of compromised systems (a botnet) attack a single target. This causes a denial of service for genuine users of the targeted system because the flood of incoming messages forces it to shut down. DDoS attacks are easily executed on a large network and can be very effective. These attacks can be directed at any networked device: routers (effectively targeting an entire network), servers (Web, mail, DNS), or specific machines (firewall, IDS) (Tanase, 2010).

DDoS attacks happen by first exploiting a vulnerability that exists on a computer system by using an automated software known as an autorooter and installing a DDoS software package. This software allows an attacker to remotely control the compromised computer. From this master system the hacker can then identify and communicate with

other systems, which will ultimately be compromised. With a single command, the controlled machines will launch one of many flood attacks against a specified target. This barrage of packets to the target is what causes a denial of service. When used for one purpose, “a single machine can generate several megabytes of traffic. Several hundred machines can generate gigabytes of traffic. With this in mind, it’s easy to see how devastating this sudden flood of activity can be for virtually any target” (Tanase, 2010, para. 6).

Past Attacks

In April, 2000, a former contractor with the company that installed a computerized sewage system for Maroochy Shire Council in Queensland, Australia, was enraged after being denied a permanent job. To get even, he “hacked into the sewage system and released up to 1 million liters of raw sewage into public parks, creeks, and a hotel, severely polluting the environment” (Rege-Patwardhan, 2009, p. 264). On at least 46 occasions he issued radio commands to the sewage equipment. Marine life died, the creek water turned black and the stench was unbearable for residents.

The attacker in this incident had several advantages. First, he had insider knowledge that he used to access the sewage system from his car. He did this using his laptop to connect to the SCADA equipment. Second, he knew he could exploit the system because it was using inadequately protected wireless communication. His contractor credentials were not terminated upon completion of the installation, which enabled his attack. Furthermore, over the three months that he was connecting to the system, his hacking attempts went unnoticed.

In 2001, hackers successfully attacked an electric power grid in California. They attempted to breach the computer system at the California Independent System Operator (Cal-ISO). Cal-ISO balances the flow of electricity across the state of California and makes power purchases to meet the demand. Cal-ISO is also responsible for assisting electric companies in avoiding blackouts. The attack on Cal-ISO began in late April, lasted for at least 17 days, and was not detected until the second week of May. It was traced back to the "Guangdong province of China, which had created many of the malicious worms and Trojan horse attacks" (Rege-Patwardhan, 2009, p. 264).

The attack took place while rolling blackouts swept through California on May 7 and 8, affecting over 400,000 utility customers. Cal- ISO officials asserted that the attack had nothing to do with the blackouts that were experienced. "'This was very close to being a catastrophic breach,' said a source familiar with the attack and Cal-ISO's internal investigation of the incident." (Morain, 2001, para. 8).

An internal investigation uncovered that hackers gained access to two Solaris Web servers that were part of a development network and were not behind the network's firewall. Essentially the servers were connected directly to the Internet and were configured with default settings, making them extremely vulnerable to an array of attacks. It appeared that hackers had gained access through a Solaris vulnerability that had not been patched. After gaining access to the servers, hackers installed a root kit in an attempt to get from the development network into more sensitive areas of Cal-ISO's network. But because audit logs were not sent to other systems, it could not be trusted that the local logs had not been modified, thus making it impossible to uncover further details.

Baltimore's Constellation Energy Group, Inc. has experienced hundreds of hacker intrusions on a daily basis. "While the company's security team noted that no serious damage had occurred, and the source of attacks remained unknown, the untiring efforts of hackers generated immense fears about widespread blackouts" (Rege-Patwardhan, 2009, p. 264). It was also reported in 2009 that hackers planted malicious software in the U.S. electric grid and other critical infrastructures like telecommunications networks, and in computer systems of the financial services industry. The code in the electric grid was discovered around 2006 or 2007, according to an official who likened it to an updated version of spying. "Although these attacks were narrower in scope and magnitude than the hypothetical scenario, they each demonstrate the vulnerability of critical U.S. infrastructure" (Gable, 2010, p. 2).

Officials believe that cyber spies came from China, Russia, and other countries, and were most likely trying to navigate the U.S. electrical system and its controls. The espionage appeared pervasive across the U.S. and did not target a particular company or region, said a former Department of Homeland Security official (Gorman, 2009). Authorities investigating the intrusions found software tools left behind that could be used to destroy infrastructure components. And even though the intruders did not damage the power grid, officials warned they could try during a crisis or war (Gorman, 2009).

First reported in June 2010, the Stuxnet worm gained notoriety a month later when Microsoft confirmed that it was actively targeting Windows computers that managed SCADA systems. Stuxnet was transferred to computers via an infected USB device and could use four different unpatched or "zero-day" vulnerabilities in Windows to gain administrative access to corporate networks. From there the worm would seek out

and infect the computers that managed SCADA systems controlled by software from Siemens, a German electronics company. The worm would attempt to use default Siemens passwords to take control of the SCADA software and reprogram the machine with new instructions. The attack also involved theft of a signed digital certificate owned by Realtek Semiconductor, to authenticate drivers needed by Stuxnet when it self-installs.

Stuxnet was written in multiple languages, including C, C++, and other object-oriented languages. "Someone had to sit down and say, 'I want to be able to control something on the factory floor, I want it to spread quietly, I need to have several zero-days,' and then pull together all these resources." (Keizer, 2010, para. 12). The creators of Stuxnet also put a counter in the infected USB device that minimized the chance of discovery by allowing the worm to spread to no more than three computers. This help contain it to the target facility (Keizer, 2010).

Information Sharing

Approximately 90% of the nation's critical infrastructures is privately owned and operated. This means the private sector is often in the best position to share relevant information with the federal government, specifically the Department of Homeland Security (DHS), about securing critical infrastructures. "Frequently, DHS cannot gain information regarding a critical infrastructure's choke points, protection strategies, or response plans unless the owner of the facility voluntarily shares the information with the Department" (Whitley et al., 2007, p. 272).

Attacks on the private and public infrastructures of the U.S. are now linked with the national security of the country more than ever before. For this reason, the ability for the nation to defend against a cyber attack hinges on information sharing between private

industry and government. Information sharing may assist the government in establishing a process to identify an ongoing attack.

Prior to a statutory amendment of the Freedom of Information Act (FOIA), owners and operators of critical infrastructures were reluctant to share pertinent information with the federal government for fear that competitors, or even terrorists and criminals, would use FOIA to compel the federal government to share what otherwise would not have been in the public domain but for voluntary disclosure. Now, the private owners and operators are able to share homeland security related information with DHS without fear of FOIA disclosures. But despite the protection from FOIA, information flow from the private sector remains slow.

It is thought that private industry continues to withhold information from the federal government for two reasons. First, that FOIA protection is not automatic. A series of steps outlined in the Code of Federal Regulations must be followed in order to obtain the protection and many view these steps as being too cumbersome (Whitley et al., 2007). Second, private industry is concerned that mistakes could be made, resulting in shared information being released accidentally. A disclosure of this nature could embarrass or even damage the party who offered the information in good faith and with the expectation that it would be protected. In many cases, this concern is strong enough to deter full disclosure.

Economic Impact

An attack on the electric grid could negatively impact the local, regional, national, or even global economy. Reduced electricity would affect almost every aspect of the economy. It could hamper manufacturing plants and service producing establishments,

hinder transportation and distribution of goods, and impede the sales and delivery of a wide range of business, personal, and government services. Studying the frequency and costs associated with attacks is hindered by the reluctance of organizations to make public their experiences with security breaches.

When a power failure occurs, one of the industries most immediately affected is the banking and financial services sector. The financial industry is heavily reliant on computer networks, telecommunications, and wireless technology. This dependency results in an immediate degradation of services after a collapse of the electrical grid. Computers are an important contributor to efficiency in financial industries and many companies have safety measures in place to provide emergency power backup via uninterrupted power supplies (UPS) or generators in an effort to avoid data loss and damage to computer hardware (Abernathy, 2003). Emergency power backup allows banking branches and service centers to maintain some services at a minimal level to help prevent lost or forfeited transactions. Financial firms' regulators have issued requirements for redundancy and security in the physical and financial systems that support operations. The regulations force most institutions to have multiple types of back-up systems and data backups that assist in recovery of applications and business recommencement (Federal Financial Institutions Examination Council [FFIEC], 2010).

A failure in the electric grid may cause financial panic amongst the general public. Financial institutions not only operate on confidence, but they also promote confidence. It is important for financial institutions to continue to operate as closely as possible to business as usual. Allowing the public to engage in uninterrupted business helps to keep markets stable during times of stress. In 2003, Financial and Banking

Information Infrastructure Committee representative Wayne Abernathy testified in front of the U.S. House of Representatives, verifying that financial institutions must provide confidence to help cope with the trauma of a disaster, “confidence that financial transactions will be carried out, that checks will clear, that bills will be paid, that investments will be made, that insurance promises will be kept” (Abernathy, 2003, p. 2).

From the consumers' point of view, the major impact of an electrical failure is access to monetary funds via automated teller machines (ATM). If a bank has a backup generator, some ATM machines are able to operate while battery power is available. Consumers in general are not unused to experiencing some kind of disruptions with respect to access to ATM machines. However, in the case of a lengthy outage, ATM machines will cease to operate once backup power sources have been depleted. The public should be educated and prepared for situations like this. Without an emergency plan, how will the public access their money? Many people rely on ATMs on a regular basis for cash to purchases goods and services, and should have an emergency stash of cash for emergencies.

A study conducted by Berkeley Lab researchers for the U.S. Department of Energy’s Office of Electric Transmission and Distribution estimates that electric power outages and blackouts cost the nation about $80 billion annually. The Berkeley Lab study combined data from three sources: surveys on the value electricity customers place on uninterrupted service, information recorded by electric utilities on power interruptions, and information from the U.S. Energy Information Administration on the number, location and type of U.S. electricity customers (Chen, 2005). The study estimates the total cost to the U.S. of power interruptions at about $80 billion per year – $57 billion (73

percent) in losses from the commercial sector and $20 billion (25 percent) in losses from the industrial sector. The authors estimate residential losses at $1.5 billion, or 2 percent of total losses. “It is difficult to put a dollar value on the inconvenience or hassle associated with power interruptions affecting residential electricity customers” (Chen, 2005, para. 7).

Anderson Economic Group estimated the cost of a blackout in 2003 to have a total economic cost of between $4.5 and $8.2 billion. This includes $4.2 billion in lost earnings for workers and investors, $15 to $100 million in extra costs to government agencies due to overtime and other emergency service costs, $1 to $2 billion in costs to the affected utility companies, and between $380 and $940 million in costs associated with lost or spoiled commodities (ELCON, 2004). The U.S. Department of Energy (DOE) published a total cost for the 2003 blackout as an estimated $6 billion (ELCON, 2004).

Another study completed after the 2003 blackout by the Ohio Manufacturers’ Association (OMA) estimated the direct costs of the blackout on Ohio manufacturers to be $1.08 billion. All companies that participated in the study indicated that the blackout caused a complete shutdown in operations (ELCON, 2004). The OMA survey confirms that a blackout’s economic cost may reasonably be measured in the billions of dollars.

Prevention & Protection

With so many challenges to critical infrastructure protection, it is crucial to determine how to begin a proactive protection strategy. Risk management may be the most appropriate model for critical infrastructure protection. Under a risk management strategy, “possible targets are analyzed according to a combination of three metrics:

threat, vulnerability, and consequence. Sites with a high threat level that are especially vulnerable to an attack that would result in severe consequences would receive the greatest protection" (Whitley et al., 2007, p. 278).

Risk management involves deciding which protective measures to take based on an agreed upon risk reduction strategy (Moteff, 2004). Many models and methodologies have been developed by which threats, vulnerabilities, and risks are integrated and then used to inform the cost-effective allocation of resources to reduce those risks. For the most part, these methodologies consist of the following elements, generally performed in the following order:

- Identify assets and identify which are most critical
- Identify, characterize, and assess threats
- Assess the vulnerability of critical assets to specific threats
- Determine the risk or expected consequences of different types of attacks on those assets
- Identify ways to reduce those risks
- Prioritize risk reduction measures based on a strategy

A risk management program is critical for a critical infrastructure provider to successfully implement and maintain an acceptable level of security. The benefits of risk management are often effective strategic planning, fewer costly surprises by preventing what is undesirable from occurring, and better outcomes in terms of program sustainability, effectiveness, and efficiency. Effective risk management will also contribute to improved security governance (Commonwealth of Australia [Commonwealth], 2005).

Government and private industry have also been working together to develop international standards to help prevent cyber attacks. To provide adequate security, not only must the information being transmitted be secure, but the communicating parties also need to be authenticated to ensure they are truly the persons they claim to be. Thus, data integrity, encryption, and authentication are vital to the protection of crucial infrastructures.

Data integrity. To provide adequate security, data integrity must be ensured. PC Magazine's (2011) Encyclopedia defines data integrity as the quality of correctness, completeness, wholeness, soundness, and compliance with the intention of the creators of the data. The organizations that control the nation's critical infrastructure should consider explicitly the risks associated with data integrity. The concern is that attackers could access sensitive data not just to read it, but to alter it with the intention of undermining the ability to transact business or produce accurate reports. This shows an increased reliance on electronic data, and may call for an increased need for integrity of sensitive data. "The need for both data integrity and authentication significantly compounds the security structures to be implemented and maintained" (Gable, 2010, p. 34).

Encryption. Data integrity concerns may typically be resolved through the use of encryption. Encryption protects data by decoding it so that if intercepted it will be undecipherable. Even strong encryption methods are not fool-proof, however. "Encryption is most effective in countering password-sniffing, snooping, and eavesdropping, but is absolutely useless in preventing the injection of malicious code, spoofing, and tampering, to name but a few other types of attacks" (Gable, 2010, p. 35). Encryption essentially only protects the data itself, not the network over which the data is

being sent, the system that the data originated from, or any other information on the Internet.

Encryption sometimes allows a network to stay just one step ahead of attackers. Hackers and terrorists are constantly looking for new and innovative ways to attack computer systems. It is a struggle for both government and private industry to stay ahead of them, proving that the industry is in a reactionary position. “Although better and stronger forms of encryption are constantly being developed, the search for stronger encryption appears to be never-ending, because each increase in encryption strength seems to be matched by an advance in decryption” (Gable, 2010, p. 37).

While encryption helps to secure the data, another issue that needs to be addressed is the security of the networks and communication channels over which the data is sent. “Protecting these other aspects of the network is much more difficult, as a result of both the basic flaws in the infrastructure of the Internet and the transparency of information available via the Internet” (Gable, 2010, p. 35). Attackers stake out these communication channels looking for ways to intercept and decipher the data being sent over it, and this partially impairs the ability to ensure data integrity.

Authentication. Authentication is the process of ensuring the identities of the communicators. Authentication concerns may be mitigated to some degree through the use of methods to validate both the source and content of information and the identity of users during the login process. The two most common methods of authentication are passwords and digital signatures (Gable, 2010).

Passwords are a means of identifying the user of a system, as they are unique to each user, but they are not always secure. The time it takes to crack a password is related

to the password's strength, so the use of complex passwords makes it harder for an attacker to guess the password. The most effective type of password is the one-time password, which "generally is not susceptible to password guessing… due to the sheer effort that is involved–if a password is a six-digit number that changes randomly each minute, an attacker has one chance in a million of guessing the password" (Gable, 2010, p. 35).

Common methods used to crack passwords are dictionary attacks and brute force attacks (Shimonski, 2002). A dictionary attack involves entering every word in a dictionary as a password in an attempt to break into a system. Individuals tend to choose passwords that are simple, such as short words found in dictionaries, which can be easily predicted. A brute force attack is similar to a dictionary attack in that it tries every possible combination of options of a password. This type of attack may take a long time to complete because complex passwords are harder to identify.

Digital signatures may also be effective in determining someone's identity. A digital signature is a "form of public-key cryptography that adds an electronic signature to the end of a message or file, proving that the person who claims to have sent it actually did so" (Gable, 2010, p. 35). If a message is digitally signed, any change made to the message after it is signed will invalidate the signature.

United States Regulation

Congress passed the Cyber Security Enhancement Act of 2002 as part of the Homeland Security Act of 2002. The act amended the USA PATRIOT Act to loosen restrictions on Internet service providers (ISPs) as to when, and to whom, they are allowed to voluntarily release information about subscribers. The act lowered the

threshold for when ISPs may voluntarily divulge the content of communications. At this time, ISPs require only a good faith belief to release information, instead of only a reasonable belief that there is an emergency involving danger of death or serious physical injury. The contents may be disclosed to a federal, state, or local governmental entity. The act also amended the federal sentencing guidelines to address crimes involving fraud in connection with computers and access to protected information, protected computers or restricted data in interstate or foreign commerce or involving a computer used by or for the federal government.

The Critical Infrastructure Information Act of 2002 exempts information voluntarily submitted by private owners and operators of critical infrastructure from the Freedom of Information Act and other federal and state disclosure requirements. The information generally disclosed by these companies is for government use regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, or other informational purpose (Library of Congress, 2004).

The National Strategy to Secure Cyberspace of 2003 aims to reduce the vulnerabilities presented by the Internet, prevent cyber attacks against U.S. critical infrastructures, reduce vulnerability to cyber attacks, and minimize damage and recovery time from successful cyber attacks. “The 60-page document recognized that our economy and national security are dependent upon the Internet, the core of our information technology and the information infrastructure. This infrastructure controls everything from electrical grids to stock markets” (Hoar, 2005, p. 6). In the executive summary, the role that the Internet plays in our everyday lives was appropriately described, it states:

> Our Nation's critical infrastructures are composed of public and private institutions in the sectors of agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping. Cyberspace is their nervous system—the control system of our country. Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work. Thus, the healthy functioning of cyberspace is essential to our economy and our national security. (White House, 2003, p. vii)

The strategic objectives of the national strategy are to prevent cyber attacks against U.S. critical infrastructures, reduce national vulnerability to cyber attacks, and minimize damage and recovery time from successful cyber attacks. The strategy goes on to state five critical priorities. They are: (1) the development of a national cyber space security response system, (2) the development of a national cyber space security threat and vulnerability reduction program, (3) the development of a national cyber space security awareness and training program, (4) securing the cyber space of local, state, and federal government, and (5) strengthening national security and international cyber space security cooperation (White House, 2003).

The Energy Policy Act (EPA) of 2005 is a federal statute that created homeland security responsibilities for the energy sector. Prior to the enactment of the EPA, cyber security protection for the grid was ineffective because compliance with voluntary cyber security practices requested by the NERC had been unenforceable (Whitley et al., 2007).

Title XII of the EPA, also known as the Electricity Modernization Act of 2005, states that the owners and operators of the electric power grid must ensure grid reliability.

The act "tasks the Federal Energy Regulatory Commission (FERC) to designate a new Electric Reliability Organization (ERO) to promulgate and enforce mandatory grid reliability standards" (Whitley et al., 2007, p. 277). In 2006, the FERC certified the North American Electric Reliability Council as the ERO in charge of producing reliability standards that must incorporate "requirements for the operations of existing bulk-power system facilities, including cyber security protection . . . ." (Electricity Modernization Act, 2005, para. 4).

The Cybersecurity Act of 2009 includes direction for the President to establish a Cybersecurity Advisory Panel. The panel will facilitate collaboration between the owners and operators of critical infrastructure and the government. As part of this collaboration they need to "develop and rehearse detailed response and restoration plans that clarify specific roles, responsibilities, and authorities of government and private sector actors during cybersecurity emergencies" (Shaw, 2010, para. 4). The act also requires the Department of Commerce to:

> Serve as the clearinghouse of cybersecurity threat and vulnerability information and to develop and implement a system to provide cybersecurity status and vulnerability information regarding all federal information systems and networks managed by the Department of Commerce, and would require the Director of National Intelligence and the Secretary of Commerce to submit to Congress an annual report on cybersecurity threats to and vulnerabilities of critical national

information, communication, and data network infrastructure. (Gable, 2010, p. 30)

In 2010, a bill was passed as an update to the Cybersecurity Act of 2009. Named the Cybersecurity Act of 2010, it limits authority previously given to the President to shut down private sector or government networks in the event of a cyber attack capable enough to cause massive damage.

Australian Regulation

The Australian government believes that the ideal way to enhance the resilience of its critical infrastructure is to partner with owners and operators to share information, raise the awareness of dependencies and vulnerabilities, and facilitate collaboration to address any impediments (Commonwealth, 2010). Their approach to managing the risks to critical infrastructure encourages organizations to develop a more natural ability to deal with the rapid shock created by an attack. The Australian government prefers this approach as opposed to the more traditional approach of developing plans to deal with a finite set of scenarios, especially in the context of an increasingly complex environment.

The Australian government's strategy has six complementary strategic processes to improve critical infrastructure resilience and achieve its aim and objectives:

- Operate an effective business-government partnership with critical infrastructure owners and operators
- Develop and promote an organizational resilience body of knowledge and a common understanding of organizational resilience
- Assist owners and operators of critical infrastructure to identify, analyze and manage dependencies

- Provide timely and high quality policy advice on issues relating to critical infrastructure resilience
- Implement the Australian government's Cyber Security Strategy to maintain a secure, resilient and trusted electronic operating environment, including for critical infrastructure owners and operators, and
- Support the critical infrastructure resilience programs delivered by Australian States and Territories, as agreed and as appropriate.

The Trusted Information Sharing Network for Critical Infrastructure Protection (TISN) was created by the Australian government in 2003 to provide a secure forum for owners and operators of critical infrastructure and government stakeholders to share information and discuss critical infrastructure protection issues. The TISN is Australia's primary method of building a partnership between business and government for critical infrastructure resilience. Participation in the TISN is voluntary and any information disclosed is at the discretion of each private participant that signs a deed of confidentiality (Corones & Lane, 2010).

The government has also committed to partnering with business to address cyber security initiatives through the work led by CERT Australia. The response team provides businesses with information and advice on updated threats and vulnerabilities and acts as the national coordination point in the event of a major cyber security incident. Through its work with the private sector, CERT Australia aims to make sure that the systems managed by businesses to provide everyday services are safe and secure (Commonwealth, 2009). They also engage with other CERTs internationally, and led

Australia's participation in the multinational Cyber Storm III exercise where organizations faced simulated cyber attacks.

The Critical Infrastructure Protection Branch of the National Security Resilience Policy Division within the attorney general's organizational structure develops national policy on critical infrastructure resilience and coordinates aspects of critical infrastructure policies between all levels of government. This branch is also charged with managing the TISN network. The different sections of this branch develop policies for enhanced resilience of critical infrastructure, facilitate the relationship between government and private industry, and promote consistent application of security policies and advice in Australian government agencies (Commonwealth, 2009). A 2011 project for the Protective Security Section is a review of the country's Cyber Security Strategy and publishing the findings.

The Australian government believes that their focus of engaging with the owners and operators of critical infrastructure provides substantial benefits to critical infrastructure businesses in each sector due to shared risk. Their philosophy is that "by working together on common issues, businesses within a sector, and across sectors, can enhance their resilience to various hazards" (Commonwealth of Australia, 2010, p. 10). This philosophy may also bring critical infrastructure sectors together in a non-competitive environment to discuss and address vulnerabilities.

Research Design and Methodology

The purpose of this study was to explore the cyber based threats associated with the U.S. electric grid and the programs in place to mitigate them. Research into the methods of past attacks may help to identify where networks and computer systems

might be strengthened. The cyber health of the U.S. will be analyzed along with that of Australia as well as how both countries protect their infrastructure. This research will explore if there is a need for the public and private sectors to form a partnership in regards to the cyber security of critical infrastructure, specifically the electrical grid.

Research of the U.S. electric grid will be limited in scope to the northeastern region, where the North American Electric Reliability Corporation's Critical Infrastructure Program efforts to improve physical security and cyber security for the bulk power system of North America. The Northeast Power Coordinating Council (NPCC) carries out the compliance enforcement for the NERC. The NPCC's geographic area includes New York and the six New England states (NPCC, 2011).

The project methodology was primarily a case study. It was an in-depth examination of the electric grid's network security, that aims to understand why an attack is successful and what areas are important to review in order to improve security and reliability. The potential economic impact associated with an attack on the electric grid will also be studied to understand how it may negatively affect the way business is conducted and the way consumers obtain goods and services.

This project compared U.S. cyber health with that of Australia, and investigated how both countries protect their infrastructures. The U.S. and Australia are very similar in that most of their critical infrastructure is managed by private owners and operators. The key difference between the two lies in the fact that Australia relies on a voluntary and self-regulated industry, whereas the U.S. has moved more toward a government-regulated industry that imposes fines for non-compliance (Corones & Lane, 2010).

The project will also employ secondary data analysis that utilizes data from official sources. The government has invested resources on studying the electric grid and the vulnerabilities associated with it. They have used this data to implement policies that help to mitigate threats. As part of this research, these policies will be analyzed to determine how they affect the overall security of the grid. The documents reviewed for this paper included academic texts and journal articles, magazine and newspaper articles, and government press releases from 1999 to 2011.

Discussion of the Findings

The research uncovered two key differences in the cyber health and security strategies of the U.S. and Australia. The first being the way in which the infrastructures are protected and secured. The U.S. focuses on structured regulatory compliance, whereas Australia's TISN network is not mandatory and neither is reporting of breaches. Compliance and sanctions are important when securing a critical component of the economy and nation. If properly implemented, it may help to ensure that the best interests of society are being taken into account and prove the critical impact that emerging cyber threats may have.

The second key difference is the potential liability facing the critical infrastructure owners and operators for not having structured information security governance implemented. The U.S. imposes fines and sanctions along with a public announcement of noncompliance that may blemish an offender's reputation. On the other side of the spectrum, however, Australia neither makes it mandatory to inform government of breaches, nor do they have a program in place to audit the security governance of owners

and operators. The government seems to have placed their faith in the private industry and does not see a need to be more hands on and authoritative.

Infrastructure Protection: U.S. vs. Australia

U.S. electric utility companies must comply with NERC cyber security standards. NERC is authorized by the federal government to enforce compliance to these standards, and all companies were expected to be fully compliant with these standards by 2010. The nine standards set forth under this program are called Critical Infrastructure Protection standards or NERC CIP-001 to CIP-009. CIP standards are in total made up of about 47 requirements and 100 sub-requirements. The standards are as follows:

- CIP-001 – Sabotage reporting
- CIP-002 – Critical cyber asset identification
- CIP-003 – Security management controls
- CIP-004 – Personnel and training
- CIP-005 – Electronic security perimeters
- CIP-006 – Physical security of critical cyber assets
- CIP-007 – Systems security management
- CIP-008 – Incident reporting and response planning
- CIP-009 – Recovery plans for critical cyber assets

The federal government relies on the standards enforced by NERC to assure that the core electric grid in North America will not fail due to cyber related vulnerabilities and attacks. Hayden (2009) states that the overriding goal of CIP-002 through CIP-009 is to ensure the bulk electric system is protected from unwanted and destructive effects caused by cyber terrorism and other cyber attacks, including attacks from within the

utility (i.e., insider threats). Compliance for these standards are measured by: annual self-certification, spot check audits that may be performed at any time with up to thirty days notice, periodic audits to be scheduled once every three years, and triggered investigations made within sixty days of an event or complaint of noncompliance. The individual standards are detailed below based on information available through NERC's web site (http://www.nerc.com).

CIP-001: Sabotage reporting. Companies must have procedures in place to identify disturbances or unusual occurrences whether they are suspected of sabotage or determined to be caused by sabotage. These procedures include identifying the activity, triaging to determine if it is sabotage, and reporting the activity to the appropriate systems, governmental agencies, and regulatory bodies. Compliance is measured against having properly documented procedures for the recognition of an occurrence, and for notifying the proper entities, as well having a documented communication contact list.

CIP-002: Critical cyber asset identification. Managing and maintaining a reliable electric system increasingly relies on cyber assets supporting critical reliability functions and processes for services and data. This results in increased risks to these cyber assets. Companies must start by understanding what their critical assets are.

Critical assets are the facilities, systems and equipment which, if destroyed, degraded or otherwise rendered unavailable, would affect the reliability or operability of the bulk electric system. These assets normally include items like system control centers, large generation facilities and critical substations. Risk-analysis is used in determining which assets are critical. Critical cyber assets are considered those having at least one of the following characteristics: uses a routable protocol to communicate outside the

electronic security perimeter; uses a routable protocol within a control center; or is dial-up accessible. Senior management must conduct an annual approval of the risk-based methodology, list of critical assets and the list of cyber critical assets with documentation being retained from previous full calendar year.

CIP-003: Security management controls. This standard requires that companies have minimum security management controls in place to protect the critical cyber assets identified in CIP-002. They are responsible for documenting and implementing a cyber security policy that represents management's commitment to securing critical cyber assets. The policy needs to be readily available to all personnel who have access to, or are responsible for, critical cyber assets.

A single senior manager has to be assigned with overall responsibility and authority for leading and managing the company's implementation of CIP-002 through CIP-009. Changes to the senior manager must be documented within thirty calendar days of the effective date. The senior manager is responsible for authorizing and documenting any exception or instance where they cannot conform to the security policy. Documented exceptions to the policy must include an explanation as to why the exception is necessary and any compensating measures. Authorized exceptions to the cyber security policy must be reviewed, approved and documented on an annual basis by the senior manager to ensure they are still required and valid. Exceptions must be documented within thirty days of being approved by the senior manager.

Companies must document and implement a program for managing access to protected critical cyber asset information. A list of personnel who are responsible for authorizing electronic or physical access to protected information as well as access

privileges must be maintained and should be reviewed annually. The processes for controlling access privileges to cyber assets must also be documented and reviewed annually. Under this standard, companies must also establish and document a change control process for adding, modifying, replacing, or removing critical cyber assets.

CIP-004: Personnel and training personnel. This standard covers training employees on how to comply with physical security access controls as well as IT security awareness training. Personnel including contractors and service vendors that have authorized electronic or authorized unescorted physical access to critical assets must have an appropriate level of personnel risk assessment, training, and security awareness. This standard ensures that all personnel are trained prior to being granted access except in specified circumstances such as an emergency.

Training must cover the policies, access controls, and procedures developed for the critical cyber assets and include: the proper use of critical cyber assets; physical and electronic access controls to critical cyber assets; the proper handling of critical cyber asset information; and action plans and procedures to recover critical cyber assets following a cyber security incident. Documentation must be maintained showing that training was conducted annually, including the date the training was completed and attendance records.

Companies must also have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws for personnel having authorized electronic or authorized unescorted physical access to critical assets. The personnel risk assessment program should, at a minimum, include an identity verification (e.g., Social Security number verification in the U.S.) and seven-year criminal check.

A list of all personnel, including contractors and services vendors, with authorized electronic or authorized unescorted physical access to critical assets, along with their specific electronic and physical access rights to critical assets must be maintained. This list of personnel should be reviewed quarterly, and be updated within seven calendar days of any change of personnel or in the access rights of such personnel. Access to critical cyber assets must be revoked within twenty-four hours of personnel being terminated and within seven calendar days for personnel who no longer require access to critical cyber assets.

CIP-005: Electronic security perimeters. This standard requires the identification and protection of the electronic security perimeter inside which all critical cyber assets are located, as well as all access points along the perimeter. Every critical cyber asset must be located within an electronic security perimeter. Any non-critical cyber asset within the defined security perimeter must be identified and protected as well. Documentation of the electronic security perimeter must be maintained as well as all interconnected critical and non-critical assets within the electronic security perimeter, all electronic access points to the electronic security perimeter and the cyber assets deployed for the access control and monitoring of these access points.

Processes and procedures for control of electronic access at all electronic access points to the electronic security perimeter must be implemented. These processes and procedures must use an access control model that denies access by default, so that exact access permissions must be specified. Only ports and services required for operations and for monitoring cyber assets within the electronic security perimeter should be enabled, and the configuration of those ports and services should be documented. Where external

access into the electronic security perimeter has been enabled, the company must implement strong controls to ensure the authentication of the accessing party.

A monitoring and logging process must be implemented and documented in regards to access at the access points to the electronic security perimeter 24 hours a day, seven days a week. The security monitoring process should detect and alert for attempts at or actual unauthorized accesses. Where alerting is not technically feasible, the company must review and assess access logs at least every ninety calendar days.

A vulnerability assessment of the electronic access points to the security perimeter must be performed annually. The vulnerability assessment should include: a document identifying the vulnerability assessment process; a review to verify that only ports and services required for operations at these access points are enabled; the discovery of all access points to the electronic security perimeter; a review of controls for default accounts and passwords; and documentation of the results of the assessment, the action plan to mitigate vulnerabilities identified in the assessment, and the execution status of said action plan.

CIP-006: Physical security of critical cyber assets. This standard ensures the implementation of a physical security program for the protection of critical cyber assets. The company is required to document, implement, and maintain a physical security plan, approved by the senior manager. All physical access points must be identified for the physical security perimeter and the measures in place to control entry at those points. Appropriate use of physical access controls must be in place including visitor pass management and prohibition of inappropriate use of controls.

A visitor control program for personnel without authorized unescorted access through the physical security perimeter must be in place and contain logs to document the entry and exit of visitors, including the date and time, and continuous escorted access of visitors within the physical security perimeter. Companies must update the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including the addition or removal of access points through the physical security perimeter, physical access controls, monitoring controls, or logging controls. The security plan must be reviewed annually.

Companies must document and implement controls to manage the physical access at all access points to the physical security perimeter, and the monitoring and logging of physical access at all points, 24 hours a day, seven days a week. Unauthorized access attempts must be reviewed and logged with sufficient information to uniquely identify individuals and the time of access 24 hours a day, seven days a week. Physical access logs must be retained for at least ninety calendar days.

The final part to this standard is the implementation of a maintenance and testing program to ensure that all physical security systems function properly. The program must include: testing and maintenance of all physical security mechanisms on a cycle no longer than three years; retention of testing and maintenance records for the cycle determined; retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year. All other documentation should be kept from the previous full calendar year.

CIP-007: Systems security management. This standard requires companies to define processes and procedures for securing both critical and non-critical cyber assets

within the electronic security perimeter. Companies must ensure that new cyber assets and any significant changes to existing cyber assets do not negatively affect existing cyber security controls. Changes would include installation of security patches, service packs, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

Test procedures must be created to minimize any adverse effects to the operation of the production system. This includes a security patch management program for evaluating, testing, and installing applicable cyber security software patches for all assets within the electronic security perimeter. Companies must also document the use of anti-virus software and other malware prevention tools to prevent the propagation of malware on cyber assets.

A process to ensure that only those ports and services required for normal and emergency operations are enabled must be established with only those ports and services required for normal and emergency operations being enabled. In the case where unused ports and services cannot be disabled due to technical limitations, compensating measures applied to mitigate risk exposure must be documented. Companies must establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

A policy must be implemented to minimize and manage the acceptable use of administrator, shared, and other generic account privileges including factory default accounts. The policy shall include the removal, disabling, or renaming of such accounts where possible. Passwords must be a minimum of six characters, consisting of a

combination of alpha, numeric, and special characters and should be changed at least annually, or more frequently based on risk.

Changes resulting from modifications to the systems or controls must be documented within thirty calendar days of the change being completed. Security–related system event logs documentation should be retained for ninety calendar days. Companies must keep all documentation and records from the previous full calendar year unless directed by its compliance enforcement authority to retain specific evidence for a longer period of time as part of an investigation.

CIP-008: Incident reporting and response planning. This standard ensures the identification, classification, response, and reporting of cyber security incidents related to critical cyber assets. A cyber security incident response plan should be developed and implemented in response to cyber security incidents. This plan should address: procedures to classify events as reportable incidents; response actions, including roles and responsibilities of incident response teams, incident handling procedures, and communication plans.

Cyber security incidents must be reported to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). Electric companies must have a process for updating the cyber security incident response plan within thirty calendar days of any changes and ensure that it is reviewed and tested annually. A test ranges from a paper drill, to a full operational exercise, to the response to an actual incident. Companies must keep documentation related to cyber security incidents reportable for three calendar years.

CIP-009: Recovery plans for critical cyber assets. This standard ensures that recovery plans are put in place for critical cyber assets and that these plans follow established business continuity and disaster recovery techniques and practices. The recovery plan must address the required actions to respond to an event or conditions of varying duration and severity that would activate the recovery plan, and define the roles and responsibilities of responders. Processes and procedures for the backup and storage of information required to successfully restore critical cyber assets should also be included. Recovery plans must be tested annually. An exercise of the recovery plan ranges from a paper drill, to a full operational exercise, to recovery from an actual incident.

Recovery plans must be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates will be communicated to personnel responsible for the activation and implementation of the recovery plan within thirty calendar days of the change being completed. All other documentation should be retained from previous full calendar year.

The NERC CIP standards adopted in the United States proves that the government's security posture is one that demands compliance and better security than the market does. It seems that "countries with the most active regulatory regimes tended to earn the most respect and confidence from private industry" (Baker et al., 2011). NERC's efforts have gone a long way to ensure the security of the U.S. electric grid.

The Australian government's approach to critical infrastructure protection goes beyond the risk management and business continuity planning of the U.S. to also address hazards and risks that may be unforeseen or unexpected. Australia's resilience approach

gives organizations the ability to effectively respond to a crisis and to learn and adapt from an event. The Commonwealth of Australia (2010) stated that a "resilience approach to managing the risks to critical infrastructure encourages organizations to develop a more organic capacity to deal with rapid-onset shock" (p. 5). Australian government prefers this method to a traditional risk management approach of developing plans to deal with a predetermined set of circumstances.

Critical infrastructure protection, or resilience as Australia tends to call it, is an ongoing process and occasional review and fine tuning of the activities under each strategic imperative will be required as the Strategy is implemented. Success isn't measured by whether companies comply with a rigid set of rules and standards but rather by the following criteria established by the Commonwealth (2010):

- Effective engagement between governments and industry, both within and outside the TISN, for the exchange of information and intelligence, and the development of solutions to relevant security issues, on a sectoral and cross-sectoral basis
- Sector groups being well supported by government and responsive to changes in the environment, individually and collectively
- Businesses and governments collaborating to develop and promote best practice in critical infrastructure resilience and resilience capabilities being integrated into everyday business activities
- The need for investment in resilient, robust infrastructure being considered in market regulation

- Businesses and governments collaborating to identify key cross-sectoral dependencies and vulnerabilities with respect to both cyber and physical infrastructure
- Businesses and governments collaborating to progress national research and development in critical infrastructure resilience
- A positive and robust relationship between the different levels of government on critical infrastructure resilience, and a level of national consistency and coordination while also supporting the different approaches of governments
- Critical infrastructure resilience issues and implications for owners and operators of critical infrastructure being considered in the Australian government policy development processes
- Lessons from exercise activities and real life events being propagated to all sector groups to enhance organizations' understanding of resilience and improve planning arrangements, and
- Owners and operators being integrated into the implementation of the cyber security strategy and having useful engagement with CERT Australia.

Because of the secrecy surrounding TISN meetings it is difficult to determine how many private owners and operators of critical infrastructure participate in the information exchange. There is no way of knowing who represents the owners and operators at the meetings–is it senior level management with decision making abilities or the technical people supporting the systems? As discussed, disclosure is not mandatory therefore it is difficult to gauge how extensive breaches are and whether or not they are being disclosed.

The traditional approach of risk management requires a comprehensive understanding of likelihood and consequence. Because of the growing complexity of critical infrastructure systems and the environments in which they operate, it is difficult for owners and operators to fully comprehend all the relevant vulnerabilities and threats. The government believes that as complexity increases, owners and operators will be forced to make decisions on increasingly imperfect information. Therefore, an approach that builds organic capacity in organizations to unforeseen risks and threats is necessary to expand the way in which all hazards are managed by critical infrastructure owners and operators (Commonwealth, 2010).

Centralized decision making is emphasized in risk management with an approach based on written plans for specific event types. This places the burden on companies to ensure they have: complete knowledge, expertise, and constant communication with responders. The Commonwealth (2010) argues that "building organizational resilience through distributed decision making, unified by a strong sense of ownership and purpose over the response priorities, and aided by adaptable tools and techniques, gives organizations improved capacity to handle both foreseeable and unforeseen events" (p. 13).

Australia's system is also referred to as scenario based planning. It plays an important part in assessing whether organizations have developed an adequate resilience capacity and have the best tools in place, but also strives to empower decision makers to see risk mitigation and response as part of their role. The philosophy is based upon the idea that tools and techniques that are part of normal business may be more successful than those that may be only used when a specific plan is activated (Commonwealth,

2010). This strategy could give organizations a greater ability to adapt to events that may have been unforeseen or excluded from planning as being very low likelihood. In this way, critical infrastructure protection is achieved not just by traditional risk management practices but also through organizational resilience initiatives.

Based on these philosophies, the Australian government generally takes a non-regulatory approach to critical infrastructure. This approach recognizes that in most cases, the owners and operators of critical infrastructure are best placed to manage risks to their operations and determine the most appropriate mitigation strategies. Although certain sectors of critical infrastructure are regulated to strengthen security and to comply with international treaty obligations, the government believes that as a general rule, regulation is not suitable for critical infrastructure because the identification of minimum security benchmarks or regulations may be difficult (Commonwealth, 2010).

Liability: U.S. vs. Australia

Energy providers are motivated to comply with NERC's CIPS standards since NERC may, and has, imposed fines for noncompliance. Enforcement actions under CIPS include correction of any issues identified where a mandatory NERC standard is not being fully met. U.S. law also requires that NERC's enforcement actions involving companies operating in the continental U.S. be filed publically with FERC, who has oversight of NERC's activities.

Any penalties or other enforcement actions become effective thirty days after the filing unless FERC chooses to review the penalty or settlement or a proceeding is initiated. Table 1 depicts NERC's penalty matrix for noncompliance. The matrix is based on the violation severity level and the violation risk factor. For example, if a company

has a severe violation with a high risk factor, it may be fined $1 million per day from the last time it was audited as being in compliance.

Table 1

NERC Penalty Matrix

	Violation Severity Level							
Violation Risk Factor	Lower		Moderate		High		Severe	
	Range Limits		Range Limits		Range Limits		Range Limits	
	Low	High	Low	High	Low	High	Low	High
Lower	$1,000	$3,000	$2,000	$7,500	$3,000	$15,000	$5,000	$25,000
Medium	$2,000	$30,000	$4,000	$100,000	$6,000	$200,000	$10,000	$335,000
High	$4,000	$125,000	$8,000	$300,000	$12,000	$625,000	$20,000	$1,000,000

Note. Amounts listed in the table may be assessed on a "per day" basis (Borkowski, 2010, p. 11).

If critical infrastructure owners and operators fail to maintain reasonable security controls they may create liability under civil and possibly criminal law. If terrorists are able to successfully attack a critical infrastructure and it results in the loss of life, "the success or failure of a subsequent lawsuit would likely hinge on the level of security and emergency preparedness undertaken by the attacked venue in light of the risk" (Whitley et al., 2007, p. 275). The National Fire Protection Association (NFPA) has published a generic standard for critical infrastructure owners and operators. NFPA 1600 outlines the requirements, procedures, and methodologies necessary to ascertain a basic level of emergency preparedness. This standard calls for companies to perform risk assessments and establish communication plans in anticipation of an emergency.

Australian critical infrastructure organizations are directly subject to a range of legal and regulatory requirements. This includes corporation, data protection, and privacy laws and legislation such as Sarbanes-Oxley if conducting business abroad (Trusted Information Sharing Network, 2007). However, there is no specific government legislation dictating how owners and operators of critical infrastructure protect their assets.

Security controls are often necessary to assist the organization's corporate governance program by ensuring compliance risk is addressed. The Trusted Information Sharing Network (2007) recommends that to ensure compliance with legal and regulatory obligations, the information security team should:

- Support the legal, audit or risk departments (as applicable) in determining appropriate information security requirements for the organization to meet compliance obligations;
- Develop information security metrics that provide validation of performance relevant to the compliance obligations; and
- Ensure procurement and contracting processes include consideration of the information security compliance obligations of the organization and the comparative satisfaction of these by considered suppliers, systems, and products.

The Australian government's laissez faire approach to securing critical infrastructure may impact the side effects felt by companies that do not have secure environments. There is no legal or monetary incentive to maintain best practices, but rather a hope that companies will work together, share information, and seek to maintain

a secure and reputation amongst the community. The many attacks that possibly go unannounced to the public and government may prove that this could be a false hope.

Future Research and Recommendations

Despite the progress that has been made in terms of securing and protecting critical infrastructure, breaches and attacks taking place around the world prove that attackers remain capable, well organized, and ahead of most well-thought-out security plans. Both the private and public sector must continue to prepare for more sophisticated attacks. Success in combating the threat to critical infrastructures may only come from a clear and unbiased assessment of what the problem is and who is involved. Security policies should consider the reality of multiple threat sources and techniques.

In Australia, because there is no mandatory disclosure, it is very difficult to persuade organizations to disclose a breach. The public often discovers that an Australian company was attacked because overseas business locations are required to disclose all attacks. The Australian government should consider the development of a solution similar to that adopted in the U.S. In 2015, the Australian government's critical infrastructure resilience strategy will undergo a comprehensive review to help ensure the policy settings remain effective. Once a review is completed, a study may then be conducted to determine if the strategy is more effective than that of the U.S., or offers any other areas of improvement.

To gain a broader perspective of how critical infrastructure cyber security is regulated on a global level, it is recommended that studies assess multiple countries, not only the U.S. and Australia. There are many reasons that variations might exist between countries in terms of critical infrastructure protection. One difference is in the role played

by government; some countries encourage security by collaboration and adopt regulations that require a high level security while others have a more limited approach. “In the end, perhaps surprisingly, the countries with the most active regulatory regimes tended to earn the most respect and confidence from private industry” (Baker et al., 2011). Due to time restraints of this research, only the U.S. and Australia were analyzed. Additional research may analyze China and Japan and how extensive or detailed their regulatory authority is over critical infrastructure protection.

The general public may not be well educated on the interdependency of the different critical infrastructures and how an attack on one could affect others. To determine how prepared citizens are in regards to financial system failures due to an extended power outage, a survey should be conducted. Questions could target consumers and business owners to assess the level confidence of their ability to access capital.

Further research into disaster recovery and business continuity of financial institutions on a global scale would help to determine how prepared the industry is for an attack against the electric grid. Different countries have different regulations and expectations for security. Research into the existence of world-wide standards and strategies or the lack-thereof would help to uncover areas of opportunity for growth and improvement.

The emergence of a threat such as the Stuxnet worm points to a substantial need for companies to acknowledge the changes present in today’s virtual world and prepare not only for traditional methods of attacks, but also for more sophisticated threats (Baker et al., 2011). In light of this, research into new technologies should be conducted before countries suffer more frequent and catastrophic cyber attacks. Research should focus on

the challenges of the changing environment and the benefits of updated threat responses that are focused on improved technologies, increased oversight of access to control systems, and effective partnerships with governments. The characteristics of these partnerships are likely to vary from country to country and range from encouragement to mandatory action, but to be most effective against emerging threats; government regulation is the best option.

Appendix A

Critical Infrastructure Interdependency

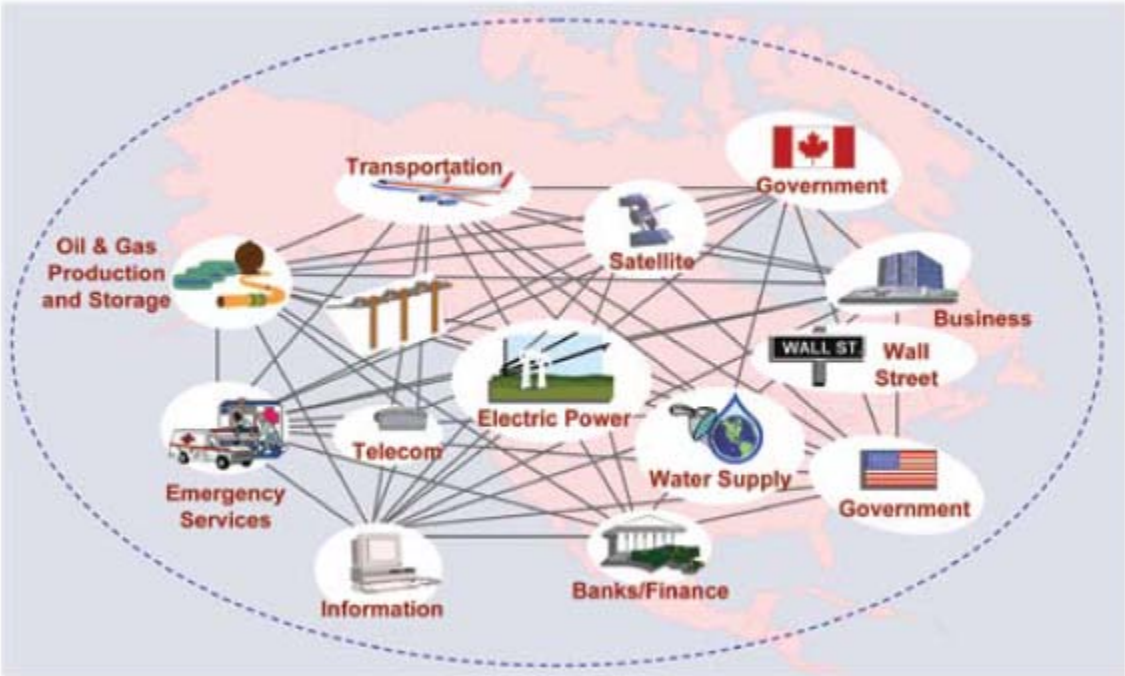

Figure 1. Interdependency of critical infrastructure. This figure illustrates the interconnectedness of the various critical infrastructures and how if one of these infrastructures is attacked, others will also be affected. Adapted from "Energy Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan," by U.S. Department of Homeland Security & U.S. Department of Energy, 2010, Retrieved from http://www.dhs.gov/xlibrary/assets/nipp-ssp-energy-2010.pdf

Bibliography

Abernathy, W. (2003). Testimony of Wayne A. Abernathy, assistant secretary for financial institutions Department of Treasury before the Subcommittee on oversight and investigations committee on financial services U.S. House of Representatives. Retrieved from http://www.scribd.com/doc/1198743/US-Treasury-backout102003

Aitoro, J.R. (2009). Electric grid breaches symptomatic of deeper cybersecurity gaps. Retrieved from http://www.nextgov.com/nextgov/ng_20090408_1423.php

Baker, S., Filipiak, N., & Timlin, K. (2011). In the dark: Crucial industries confront cyberattacks. Retrieved from http://www.mcafee.com/us/resources/reports/rp-critical-infrastructure-protection.pdf

Bataller, E. (2011).Why cybersecurity partnerships matter. Retrieved from http://www.informationweek.com/news/government/security/229301141?queryText=cybersecurity

Borkowski, M. (2010). NERC standards and compliance. Retrieved from http://www.eei.org/meetings/Meeting%20Documents/TWMS-8-Borkowski-Maureen.pdf

Chen, A. (2005). Berkeley lab study estimates $80 billion annual cost of power interruptions. Retrieved from http://www.lbl.gov/Science-Articles/Archive/EETD-power-interruptions.html

Commonwealth of Australia (2005). AusGuideline: Managing risk. Retrieved from http://www.ausaid.gov.au/ausguide/pdf/ausguideline6.3.pdf

Commonwealth of Australia (2009). Cyber security strategy. Retrieved from

http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/%284CA02151F94FFB778ADAEC2E6EA8653D%29~AG+Cyber+Security+Strategy+-+for+website.pdf/$file/AG+Cyber+Security+Strategy+-+for+website.pdf

Commonwealth of Australia (2010). Critical infrastructure resilience strategy. Retrieved from http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/%289A5D88DBA63D32A661E6369859739356%29~Australian+Government+s+Critical+Infrastructure+Resilience+Strategy.PDF/$file/Australian+Government+s+Critical+Infrastructure+Resilience+Strategy.PDF

Condron, S. M. (2007). Getting it right: Protecting American critical infrastructure in cyberspace. *Harvard Journal of Law & Technology, 20*(2), 403-442.

Corones, S., & Lane, B. (2010). Shielding critical infrastructure information-sharing schemes from competition law. *Deakin Law Review, 15*(1), 1-36.

DePoy, J., Dillinger, J., Stamp, J., & Young, W. (2003). Common vulnerabilities in critical infrastructure control systems. Retrieved from http://www.oe.netl.doe.gov/docs/prepare/vulnerabilities.pdf

Department of Homeland Security (2010). Critical infrastructure. Retrieved from http://www.dhs.gov/files/programs/gc_1189168948944.shtm

ELCON (2004). The economic impacts of the August 2003 blackout. Retrieved from http://www.elcon.org/Documents/EconomicImpactsOfAugust2003Blackout.pdf

Electricity Modernization Act (2005). Title XII – Electricity. Retrieved from http://www.nerc.com/fileUploads/File/AboutNERC/HR6_Electricity_Title.pdf

Gable, K. A. (2010). Cyber Apocalypse now: securing the Internet against cyberterrorism

and using universal jurisdiction as a deterrent. *Vanderbilt Journal of Transnational Law*, *43*(1), 57-118.

Gormon, S. (2009). Electricity grid in U.S. penetrated by spies. Retrieved from http://online.wsj.com/article/SB123914805204099085.html

Hayden, E. (2009). Getting to know the NERC CIP standards. Retrieved from http://searchsecuritychannel.techtarget.com/tip/Getting-to-know-the-NERC-CIP-standards

Hoar, S. B. (2005). Trends in cybercrime: The darkside of the Internet. *Criminal Justice*, *20*(3), 4-13.

Hoover, J.N. (2011). Cyber threats to critical infrastructure spike. Retrieved from http://www.informationweek.com/news/government/security/229401858?queryText=cybersecurity

Information Policy (2011). Cyber attacks now the most feared EU energy threat. Retrieved from http://www.i-policy.org/2011/01/cyber attacks-now-the-most-feared-eu-energy-threat.html

Jensen, E. T. (2002). Computer attacks on critical national infrastructure: A User of Force Invoking the Right of Self-Defense. *Stanford Journal of International law*, *38*(2), 207-240.

Keizer, G. (2010). Is Stuxnet the 'best' malware ever?. Retrieved from http://www.computerworld.com/s/article/9185919/Is_Stuxnet_the_best_malware_ever_?taxonomyId=85&pageNumber=2

LaMonica, M. (2010). DOE: Common security holes leave energy grid vulnerable. Retrieved from http://news.cnet.com/8301-11128_3-20012459-54.html

Lewis (2010). The electric grid as a target for cyber attack. Retrieved from http://csis.org/files/publication/100322_ElectricalGridAsATargetforCyberAttack.pdf

Library of Congress (2004). Laws and regulations governing the protection of sensitive but unclassified information. Retrieved from http://www.loc.gov/rr/frd/pdf-files/sbu.pdf

Lin, H. S. (2010). Offensive cyber operations and the use of force. *Journal of National Security Law & Policy*, *4*(1), 63-86.

McAfee (2010). Identifying and thwarting malicious intrusions. Retrieved from http://www.mcafee.com/us/resources/white-papers/wp-identifying-malicious-intrusions.pdf

Minatel, J. (2011). Malware defined, part one: Viruses, worms, and trojan horses. Retrieved from http://cws.internet.com/article/2534-.htm

Morain, D. (2001). Hackers victimize Cal-ISO. Retrieved from http://articles.latimes.com/2001/jun/09/news/mn-8294

Moteff, J. (2004). Risk management and critical infrastructure protection: Assessing, integrating, and managing threats, vulnerabilities and consequences. Retrieved from http://www.fas.org/sgp/crs/RL32561.pdf

NERC (2011). Remarks of Gerry Cauley, president and chief executive officer, North American electric reliability corporation: House homeland security subcommittee on cybersecurity infrastructure protection and security technologies. The DHS cybersecurity mission: Promoting innovation and security critical infrastructure. Retrieved from

http://www.nerc.com/fileUploads/File/News/House%20Homeland%20Security%20Subcommittee%20Cauley%20Testimony%20%20April%2015%202011.pdf

NPCC (2011). About NPCC. Retrieved from https://www.npcc.org/About/default.aspx

Obama, Barack. “Remarks on Securing Our Nation’s Cyber Infrastructure.” White House East Room Press Conference. Washington, D.C. 29 May 2009.

PC Magazine (2011). Data integrity. Retrieved from www.pcmag.com/encyclopedia_term/0,2542,t=data+integrity&i=40792,00.asp

Rege-Patwardhan, A. (2009). Cybercrimes against critical infrastructures: a study of online criminal organization and techniques. *Criminal Justice Studies: A Critical Journal of Crime, Law and Society, 22*(3), 261-271.

Sharp, Sr., W. G. (1999). Redefining national security in today's world of information technology and emergent threats. *Duke Journal of Comparative and International Law*, *9*(2), 383-389.

Shaw, D. (2010). Senate panel passes Cybersecurity Act with revised “kill switch” language. Retrieved from http://www.opencongress.org/articles/view/1773-Senate-panel-passes-Cybersecurity-Act-with-revised-kill-switch-language

Shimonski, R. (2002). Hacking techniques: Introduction to password cracking. Retrieved from http://www.ibm.com/developerworks/library/s-crack/

Stohl, M. (2006). Cyber terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games?. *Crime, Law and Social Change*, *46*(4-5), 223-239.

Tanase, M. (2010). Barbarians at the gate: An introduction to distributed denial of service attacks. Retrieved from http://www.symantec.com/connect/articles/barbarians-

gate-introduction-distributed-denial-service-attacks

Trusted Information Sharing Network (2007). Secure your information: Information security principles for enterprise architecture. Retrieved from http://www.tisn.gov.au/Documents/ITSEAG+Secure+Your+Information+CIO.pdf

US-CERT (2006). National cyber alert system: Cyber security tip ST06-001. Retrieved from http://www.us-cert.gov/cas/tips/ST06-001.html

White House (2003). The National Strategy to Secure Cyberspace. Retrieved from http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf

Whitley, J. D., Koenig, G. A., & Roberts, S. E. (2007). Homeland security, law, and policy through the lens of critical infrastructure and key asset protection. *Jurimetrics*, *47*(3), 259-279.