THE CALIFORNIA INDEPENDENT SYSTEM OPERATOR SECURITY VULNERABILITIES

Stephanie Lynn Brow
B.S., California State University, Sacramento, 2004

PROJECT

Submitted in partial satisfaction of
the requirements for the degree of

MASTER OF SCIENCE

in

CRIMINAL JUSTICE

at

CALIFORNIA STATE UNIVERSITY, SACRAMENTO

SUMMER
2010

THE CALIFORNIA INDEPENDENT SYSTEM OPERATOR SECURITY VULNERABILITIES

A Project

by

Stephanie Lynn Brow

Approved by:

_____, Committee Chair
David H. Swim, D.P.A.

_____
Date

Student: Stephanie Lynn Brow

I certify that this student has met the requirements for format contained in the University format manual, and that this project is suitable for shelving in the Library and credit is to be awarded for the Project.

_____, Graduate Coordinator _____
Yvette Farmer, Ph.D. Date

Division of Criminal Justice

Abstract

of

THE CALIFORNIA INDEPENDENT SYSTEM OPERATOR SECURITY VULNERABILITIES

by

Stephanie Lynn Brow

Statement of Problem

Our country is still in the early stages of the 21st century where technology is advancing on a daily basis allowing the threat of terrorism, both domestic and foreign, to pose a serious risk to both its citizens and its assets if not addressed soon. There are numerous potentially vulnerable sites throughout the country that are still left under guarded and under protected, specifically my emphasis for this project, the California Independent System Operator (ISO).

Sources of Data

This multilayered project utilizes public information from the Department of Homeland Security manual. The project also includes information from various national publications of defense principles and security countermeasures, as well as law enforcement protocols in place to deal with these types of security threats and potential breaches, scholarly articles, and industry trade journals.

Conclusions Reached

The California ISO lacks physical and some virtual controls that make it more vulnerable to attacks. Specific recommendations have been made to ensure that the ISO is better protected and can still run an effective business.

_____, Committee Chair
David H. Swim, D.P.A.

_____
Date

TABLE OF CONTENTS

Page

Chapter 1

INTRODUCTION

Problem Statement

The topic of study for this project will include an analysis of on-site security, needed both physically and virtually, to protect the critical infrastructure of both private and national resources of the United States of America. There are resources that are currently under protected that include key functions that the United States needs to survive and operate on a daily basis: nuclear power plants, chemical manufacturing sites, and central power grid control stations like the California Independent System Operator (ISO), which are vital to our way of life but are left largely unguarded and usually lightly monitored. However, domestic and foreign terrorism is evolving along with technology. Our communication lines connect us with the world, not only individually in the form of news and direct communications, but, maybe more importantly, by processing our financial transactions around the world allowing us to compete in the global market. These assets are key to our success and, as such, they need to be evaluated on a continuous basis to ensure counter-terrorism measures are up-to-date and up to the task of protecting our nation.

Our country is still in the early stages of the 21st century where technology is advancing on a daily basis allowing the threat of terrorism, both domestic and foreign, to pose a serious risk to both its citizens and its assets if not addressed soon. Almost nine years after the September 11, 2001, attacks on the World Trade Center and the creation of

the Department of Homeland Security (DHS) as a result, there are still numerous potentially vulnerable sites throughout the country that are left unguarded and unprotected (The USA Patriot Act, Preserving Life & Liberty, 2008).

Specific examples of unprotected critical infrastructure can be found here in our own California backyard at the California Independent System Operator (ISO). The California ISO controls, monitors and provides high-voltage electricity to over 30 million consumers within the state of California. Today, because their facilities are left unprotected, anyone can easily put a magnetic construction sign on the side of a van, proceed to drive said van containing mass amounts of chemicals and explosives directly through their main gate entrance and detonate it near main power grid equipment and buildings, instantly causing a blackout for over 30 million citizens in California alone for anywhere from weeks to months before power is restored after backup generators begin to run out (Alvarez 2010).

The energy blackout scenario mentioned above could easily be executed within any of the states across the nation due to the lack of security on-site. The chemicals that could be used in the execution can potentially be collected from the chemical plants all over the nation. Even after September 11, 2001, chemical plants are still not under federal regulations when it comes to onsite security (Leung, 2004). In New York City one of the largest chlorine gas plants exist, and is not secured by much more than a chain link fence which a vehicle could come through (Leung, 2004). Another of the major vulnerabilities in our infrastructure involves the glaring lack of “cyber” security. Our financial institutions are left under secured across the nation, ranging from actual banks

to online databases to ATM machines. In 2003, the FBI reported that Financial Institution Fraud is a Tier 1 priority with the growing technological advances (SANS Institute, 2003).

The key component developed in this literature review and security safeguards is a recommendation to both the ISO and Folsom Police Department. While the ISO has gone public with the proposed purchase of a new plant site and better security, their current site, which will be operated for the next few years, has little protection.

Chapter 2

BACKGROUND OF STUDY

Literature Review

Site Security Plan

The Department of Homeland Security, in their Risk Based Performance Standards Guidance document, discusses securing and monitoring the perimeter of a facility. "The 'Restrict Area Perimeter' addresses the need to provide for a controlled perimeter surrounding the facility or, optionally, the critical assets only if the restricted area is defined to be less than the entire facility" (Risk-Based Performance Standards Guidance, 2009). If the critical assets are confined into a smaller area within the building then the perimeter is the area directly surrounding those assets. Restricting the perimeter reduces the possibility of persons who are unauthorized accessing the facility for malicious purposes. By securing and monitoring the perimeter of a facility, personnel can easily and effectively control who enters and leaves the facility by both foot and vehicle. They are also more able to detect, delay, and defend against and respond to individuals and/or groups who obtain or have the ability of obtaining unauthorized access (Risk-Based Performance Standards Guidance, 2009). A secure perimeter also helps to deter trespassers from gaining access to the facility and will even deter possible attackers from launching attacks from nearby areas. To restrict the perimeter access, there are two elements involved: 'securing' the restricted area and 'monitoring' the restricted area (Risk-Based Performance Standards Guidance, 2009). Securing the perimeter simply

means to physically limit the accessibility of the facility. This can usually be done by the use of one or more layers of physical barriers such as fences, natural barriers and guards. Monitoring the perimeter speaks to the need to have an area awareness of the perimeter. This includes the areas immediately beyond the perimeter as well as the areas inside the perimeter. Effective monitoring can be accomplished by the use of electronic surveillance systems and intrusion detection systems that are integrated with these surveillance systems. It is also important to have an on-site security force that can monitor the facility to deter, detect, communicate and evaluate the presence of people who are not authorized along with any unauthorized activities (Risk-Based Performance Standards Guidance, 2009).

There are a number of ways to protect the facility's perimeter that the Department of Homeland Security discusses within its Risk-Based Performance Standards Guidance. These perimeter barriers provide both physical and psychological deterrents to unauthorized individuals (Risk-Based Performance Standards Guidance, 2009). "When determining what protective measures to apply to meet the Restrict Perimeter Access performance standard, a facility might consider the following potential attack scenarios: assault team, maritime, sabotage, standoff, theft/diversion, vehicle born improvised explosive devise (VBIED) (Risk-Based Performance Standards Guidance, 2009). Barriers that can be used to support this access include things such as the following: human barriers (fences, gates), vehicle barriers (berms, bollards), natural landscaping barriers (rocks, water and hedge rows) and walls (brick, cinder, concrete). These types of barriers control and restrict the area by controlling access to vehicles and people,

providing a way to channel facility entry-control points, delaying forced entry and protecting critical assets (Risk-Based Performance Standards Guidance, 2009).

Monitoring and detection equipment are key elements of effective perimeter security plans. "Often facilities will monitor for security events through a combination of human oversight and one or more electronic sensors or other intrusion detection system (IDS) components interfaced with electronic entry-control devices and alarm reporting displays" (Risk-Based Performance Standards Guidance, 2009). What usually takes place during this monitoring phase is there is an alarm that notifies the security personnel who would then either send an officer over to the area of interest or go to the camera system to check the area remotely. Some possible and effective configuration of an IDS might include fence mounted or open area sensors (vibration detection sensors, video motion detection), remote surveillance (Closed Circuit Television (CCTV) cameras, Internet Protocol (IP) cameras), and then human-based monitoring (Risk-Based Performance Standards Guidance, 2009). In order to increase the reliability, one can choose to have many redundant sensors or countermeasures at high–risk locations.

The Department of Homeland Security discusses the importance of lighting at a facility and the deterrent it presents (Risk-Based Performance Standards Guidance, 2009). Lighting can help deter attempts at gaining access to a facility, but it can also help with the monitoring and detection of any attempts to gain unauthorized access. Poor lighting makes it difficult for security personnel and cameras to monitor the area and spot any possible breaches. With the appropriate amount of lighting, it deters adversaries from attempting to breach the perimeter (Risk-Based Performance Standards Guidance,

2009). Again, when choosing the lighting for facilities, there are many things that the owner/operator must take into account to ensure that it allows for the right level of protection for that specific facility.

Another area that can be discussed regarding security for a facility is the use of protective services. These services are used to enhance perimeter security. Protective services can be used in any number of ways depending on the facility's needs. An example of how these services can be used in order to deter would include standing post, monitoring critical assets by using remote surveillance and roving patrols (Risk-Based Performance Standards Guidance, 2009). It is usually necessary to use this type of patrol with another measure discussed previously to ensure that the appropriate level of security is obtained.

Security considerations made by the Department of Homeland Security include using layered security and/or combining barriers and monitoring to increase delay (Risk-Based Performance Standards Guidance, 2009). The Department of Homeland Security found that adequate perimeter security is rarely achieved by only utilizing one of the devices discussed above, but instead it is the use of multiple devices, otherwise known as "layers of security" (Risk-Based Performance Standards Guidance, 2009). This layering of security can be done in many different ways. For example, "Incorporating different types of security measures (integrating physical protective measures, such as barriers, lighting and electronic security systems, with procedural security measures, such as procedures guiding how security personnel should respond to an incident), using multiple lines of detection to achieve protection-in-depth at critical assets, and using

complementary sensors with different means of detection (CCTV and an intrusion detection system) to cover the same area" (Risk-Based Performance Standards Guidance, 2009). When deploying the security measures, one has to make sure that everything is taken into account, i.e., environment, surroundings, etc., to ensure that the facility is secure at all times and on all levels.

Since the September 11th attacks on the U.S., there has been a need to take a second look at our on-site security needed both physically and virtually to protect the critical infrastructure of both private and national resources of the U.S. There are multiple infrastructures that are currently unprotected which are needed for the U.S. to survive and operate on a daily basis (Moteff & Parfomak, 2004). Chemical manufacturing, nuclear plants and the central power grid are all vital infrastructures and go lightly guarded and largely unprotected. Infrastructures such as these are an example of assets that are key to the United States' success and need to be evaluated on a regular basis and analyzed to the utmost degree to ensure that the ISO is up-to-date with our counter-terrorism measures and protecting of these infrastructures.

In the Congressional Research Service (CRS) report for Congress, one of the many definitions of a critical infrastructure is "those systems and assets both physical and cyber so vital to the nation that their incapacity or destruction would have debilitating impact on national security, national economic security, and/or national public health and safety" (Moteff & Parfomak, 2004). The Homeland Security Act also formally introduces the concept of "key resources," which are defined as "publicly or privately controlled resources essential to the minimal operations for the economy and

government" (Moteff & Parfomak, 2004). The United States' critical infrastructures are particularly important because of the functions and the services many of them provide. These infrastructures are complex systems, and the effect of a terrorist attack has the possibility of stretching beyond just the primary target and would continue far past the immediate effect. For example, if the power grid for California was struck with an attack, California and neighboring states would not only suffer immediate outages, but it would take days to pick up and piece everything back together (Alvarez, 2010). The California ISO entails many "key assets," which are defined as assets which, if destroyed, would not endanger vital systems but have a possibility of creating local disaster or damaging our nation's morale or confidence (Moteff & Parfomak, 2004). On December 17, 2003, Homeland Security Presidential Directive 7 was published which is a policy that allows Federal departments and agencies to identify and prioritize critical infrastructures protecting them from possible terrorist attacks (Moteff & Parfomak, 2004). This requires that DHS and other agencies within the federal government collaborate with appropriate private sector entities to encourage sharing of information and protecting critical infrastructures.

Many sites are similar when it comes to effective site security. In September 2006, the City of Scottsdale, Arizona, created a document that speaks to site security and ensuring that the site is secure at all times. There are nine key elements in an effective site security plan. These nine steps are interchangeable throughout different industries.

The first of the nine steps is appointing a crime prevention liaison. This person's responsibility is to consult with law enforcement and get information regarding current

criminal activity. This will then allow the facility's procedures to be updated with current crime prevention. The second step is to create an effective site security plan. This plan is essential when building a new site. However, sometimes the site is already there and this is an afterthought. Still there needs to be a plan, and it should answer questions like: What type of lighting is needed? Where will video surveillance be placed? How will valuable materials and equipment be stored? How is the facility's perimeter be secured? These are just a few of the questions that should be asked to ensure an effective security plan is in place. Step three, is working with the neighbors surrounding the facility. It is important to make connections with them and educate them so that they know what to do if they see anything suspicious around the facility. Step four, is identifying the facility's assets and property is important so that if anything goes missing, personnel will know immediately and can respond. It is best to use a numbered asset tracking system to track and inventory items at the facility. Step five, securing the perimeter is important and should be the facility's first line of defense. Securing the perimeter also includes having cameras in areas throughout the facility to monitor and observe. Step six, states that anything valuable within the site should be locked up to ensure that if there is an attack or intruder that critical assets are safe. Step seven, states that it is important that the site has controlled access. Ideally, there should be only one access point that allows for close monitoring of those coming and going. This also means posting signage that states the rules very clearly (no trespassing). Also important is knowing and maintaining up to date data of who should have access to the site and when. Step eight, infers that lighting is very important when securing your facility.

Lights act as an effective deterrent to criminal activity. Step nine the final point, discusses the importance of communicating with the employees who are on-site. Ask the individuals who are on-site to report anything suspicious. It is important to educate those who are onsite as to what the consequences are if any individual commits a crime toward the site (City of Scottsdale, Arizona, 2006).

Cyber Threats

Department of Homeland Security defines protection of cyber as, protecting against cyber sabotage of these systems: Supervisory Control and Data Acquisition (SCADA) systems, distributed control systems (DCSs), Process Control Systems (PCSs), Industrial Control Systems (ICSs), critical business systems, and other sensitive computerized systems (Risk-Based Performance Standards Guidance, 2009). Doing so is essential in managing the overall risk. Many facilities focus on the perimeter security for their facility but do not pay as much attention to the cyber threat that lies within. To effectively secure a facility's cyber system, it is necessary to have a combination of policies and practices in numerous categories: security policy, access control, personnel security, awareness and training, monitoring and incident response, disaster recovery and business continuity, system development and acquisition, configuration management, and audits (Risk-Based Performance Standards Guidance, 2009). Cyber systems can be compromised not only electronically but also physically. "Marking and otherwise restricting specific physical areas in a facility can greatly improve security when combined with a role-based security model in which all personnel know exactly where

they are allowed and where they are not" (Risk-Based Performance Standards Guidance, 2009). Important areas to focus on are control rooms, local area network rooms, server rooms, and even wiring closets. Again, it is important to use the "layers of security" when protecting cyber systems.

In an example in Molalla, Oregon, burglars stole and destroyed the Molalla water system computers. Police were looking for information regarding the break-in at the city's water treatment plant. The burglars stole the plant's system computer. The computer contained all the programming that kept the water treatment plant working on auto-pilot (Bella, 2010). Water at the time was unaffected; however, the plant had to run on manual mode and had to be controlled and monitored in-person. While this did not have a huge impact at the time, it had the potential to become a hazardous issue, which would have had a large impact on the community. Since the attack, the plant has hired a security consultant to "harden" both the water treatment plant and the sewage treatment plant against future attacks (Bella, 2010).

Another example of a security breach was in 2001, where the California ISO was a victim to hackers. At the time there was no threat to the grid, however officials state that hackers came very close to gaining access to vital parts of the system, and could have seriously disrupted the movement of electricity across the state (Morain, 2001).

Response to Security Breaches

In the event of a security breach it is important those involved internally respond and use the emergency plan in place while working with local law enforcement and first

responders (Risk-Based Performance Standards Guidance, 2009). What if there is a security breach, either cyber or physical? Emergency response within the facility refers to the response of appropriately trained individuals. Properly equipped personnel who fully understand the potential consequence of the breach or incident are needed to ensure that the response is done in a timely manner, effective actions are taken, and response plans are followed. With these things in place, there is less of a chance of a devastating attack. It is critical that facilities with high risk have a documented crisis management plan (Risk-Based Performance Standards Guidance, 2009). Things that should be included in this plan are: contingency plans, continuity of operations plans, emergency response, post incident security, evacuation, notification control and contact requirements, re-entry and security response (Risk-Based Performance Standards Guidance, 2009). These plans are helpful in a situation of a physical breach because they usually contain the agreements with off-site responder services. The plan also gives specific roles and responsibilities to security and the crisis management team to ensure that chaos does not arise. One of the biggest areas of concern is the response when something does happen. Do the personnel on-site know how to respond? It is important to be continuously training on the response plan, drilling and completing exercises around the crisis management plan (Risk-Based Performance Standards Guidance, 2009).

The Department of Homeland Security emphasizes the importance of not confusing "security response" with "emergency response." "The initial 'security response' has tactical considerations such as deter, detect and delay, whereas the 'emergency response' relates to the more traditional efforts to contain the damage and

lessen the consequences after a security event" (Risk-Based Performance Standards Guidance, 2009). If there is a security event, the facility must have the ability to respond to such an event. If the power and communications are lost, the facility must look at considering backup power for security and communications systems (Risk-Based Performance Standards Guidance, 2009). A shutdown mode should be looked at in the case that the facility needs to shut down their operations quickly. Is there another place to bring up the facility like a backup facility? Can it shut down to a less than perfect power level and still support its systems?

Having local law enforcement and first responders available to the facility's response training is key in developing and executing the emergency plan. "In addition to helping the facility prepare to take quick and decisive action in the event of an attack or other breach of security, establishing relationships with local law enforcement improves responder understanding of the facility's layout and of hazards associated with the facility" (Risk-Based Performance Standards Guidance, 2009).

One of the big concerns is facility design. The controls around the administration of the infrastructure also play a key role in response to breaches and preparing a site. A risk assessment should be done on the site, and it should include site-specific reviews of the physical security, security of data and electronic technology system, employee security, access controls around the facility, shipping/receiving, emergency response plans, policies that address breaches in security (Richmond & Nesby-O'Dell, 2002). It is important that the security plan at the facility is a part of daily operations and that all employees are well-trained and equipped to use the plan. With a large critical

infrastructure like the California ISO, it is pertinent that this training occurs so that individuals know how to respond and understand the security around them.

One cannot create a plan that works for that specific site if it is not known what threats there are. However, if a breach has occurred, there are certain steps that should be taken. Four important elements that should be taken into account during any security breach include: containment and recovery, assessment of ongoing risk, notification of breach, and the evaluation and response (Guidance on data security breach management, 2008, p.2). Containment and recovery does not just require an initial investigation, but also a recovery plan including damage limitation. This will often take input from specialists across the organization. Assessing the risks of the breach is the next step in the plan. "Perhaps most important is an assessment of potential adverse consequences for individuals, how serious or substantial these are and how likely are they to happen?" (Guidance on data security breach management, 2008, p.3). The third step in the process is the notification of the breach. The notification needs to have an apparent purpose. "Notification should have a clear purpose, whether this is to enable individuals who may have been affected to take steps to protect themselves or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with the complaints" (Guidance on data security breach management, 2008). It is important when considering who to notify to also consider what is going to be told and how the message is going to be communicated. The fourth and final step is the evaluation and response. It is just as important to examine the causes of the breach but also to examine the response to it. "If your breach was hampered by inadequate policies or a lack of a clear allocation

of responsibility, then it is important to review and update these policies and lines responsibility in the light of experience (Guidance on data security breach management, 2008, p.5). Many facilities do not have up-to-date procedures around this type of event and therefore would have a hard time recovering from it.

Terrorist Attack Preparedness

After the terrorist attacks that took place on September 11th at the World Trade Center and the Pentagon, many people became concerned about the possibility of an attack like this occurring again. Not only is there the worry of the attacks occurring again, but the worry of the impact of these attacks. There are things one can do to prepare for something unexpected such as this that will reduce the stress when an actual emergency does occur. The most important thing to do in preparation is to develop a disaster plan. There are a number of steps one must do in order to prepare for an attack such as the World Trade Center. The Literature Review goes into more detail later in the document, but the steps include: create an emergency plan, establish a meeting place and assemble a disaster supply kit (How to Prepare for a Terrorist Attack, 2010).

If the California ISO was ever attacked, there would need to be a plan in place that communicates to staff and outsiders that rely on the California ISO what the status is. In order to communicate something like this, there needs to be a place to call or email to check on individuals and/or the damage done to the facility. As far as establishing a meeting place, there needs to be a place for staff to go in case they need to continue work in order to keep the grid up and the lights on. If the entire California ISO went down,

there would need to be a place to evacuate to in order to begin rebuilding. Because of our criticality, this is something that needs to be done as soon as the meeting place is established. Disaster kits are useful because they allow you to have the necessities quickly. Again, if the California ISO is unable to function because of a disaster, many people may need to continue working and need supplies if they cannot get home or to a residence.

The California ISO works with many local law enforcement agencies, but many of them do not work closely enough to know the importance of the California ISO. One of the first things that need to be done is to call law enforcement to make them aware of the attack if they are not already aware. It is important for those responding to know the layout of the land. They need to be able to maneuver in a way that keeps people safe and is most effective to them.

Target Hardening

The U.S. is an open and technologically complex society with an almost unlimited number of potential targets and points of vulnerability. U.S. Department of Homeland Security has identified more than 168,000 public water systems, 300,000 oil and gas production facilities, and 100 nuclear power plants. A White House assessment counted 2,800 electrical plants, 590,000 highway bridges, 66,000 chemical plants, 2 million miles of pipelines, and 1,800 federal reservoirs (Zensinger, n.d., p. 1). All of these infrastructures listed previously are targets that, if not properly protected, could have a major impact on society if attacked. “Hardening critical infrastructures against

terrorist attack may be one of the most challenging responsibilities of the homeland security mission" (Zensinger, n.d., p. 1). Hardening the infrastructure is only one of the main goals of the Department of Homeland security's plan. The other goals include awareness of the threats, vulnerabilities, the potential impacts of such an attack, strengthening the nation's ability to respond and the ability to recover from an attack (Zensinger, n.d., p. 1). "Target hardening or mitigation is a process wherein a building is made into a more difficult or less attractive target" (Secure Community Network, 2005, p.1). An extreme case of target hardening would include construction of something like a bunker that cannot be penetrated; however, that is not necessary in most cases. Stopping a terrorist attack or a physical attack on a building is very difficult, and almost any building or site can be destroyed (Secure Community Network, 2005, p.1). Obviously, a building that is designed to endure an attack is less likely to actually be attacked, and if it is, usually it will suffer less damage. Typically, terrorists will choose their attacks depending on the value of the target (Secure Community Network, 2005, p.1). High value targets are places that would cause the most devastation amongst society. Some of these places include government buildings, commercial properties or any place that inflicts major emotional and economical damage (Secure Community Network, 2005, p.1). Some examples of security measures recommended for a building with 151 to 450 employees with moderate to high public contact are: guard patrol on site, visitor control/screening, shipping/receiving procedures, intrusion detection with central monitoring, CCTV, duress alarm with central monitoring, controlled utility access and annual employee security training (Secure Community Network, 2005, p.1).

Target hardening includes things like fencing, lighting as discussed previously, and landscape design. Target hardening is not something that is done only on the exterior of the building, but it also needs to be done on the interior of the building. “Consideration should be given to both interior and exterior gathering places” (Secure Community Network, 2005, p.1). Offices of essential officials should be placed somewhere in the building that is not visible from the street or by the public. It is important to use personnel as observers. When possible, place offices facing courtyards and restricted areas; that way they can see out and monitor the areas. However, these windows should be glazed so that public or anyone else with unauthorized access cannot see in but the internal personnel can see out (Secure Community Network, 2005, p.2).

Target hardening should be a strong visible deterrent which is similar to the concept of opportunity reduction (O'Connor, 2008, p.1). It comes from the word CPTED (crime prevention thru environment design) which has worked in preventing some burglaries and possible robberies. “Using the military distinction between ‘soft’(attackable from all directions) and ‘hard’ (attackable from only one direction) targets, a soft target can be hardened by armor, camouflage, mobility, co-location with a defended location, or a less humane approach such as utilizing a human shield or by placing it in a sensitive location” (O'Connor, 2008, p.1). Some facilities can even use the term “security thru obscurity,” which is making something seem like nothing (O'Connor, 2008, p.1). O’Connor talks about the “outer” and “inner” perimeter and how the inner perimeter consists of doors, safes, files, pass systems, alarms, and inspections. There is

no perfect mix that anyone has come up with. It is a matter of what fits your facility and your facility's security needs.

Most people would think that the best way to prevent crime is in terms of target hardening or fortification. "The proper design and effective use of the built environment can lead to a reduction in the fear and incidence of crime, and an improvement of the quality of life" (Prince William County Police Department). Such things as the placement of physical features, visibility around the area which is being protected is a key element. Natural access control is another design that can be used to decrease the possibility of crime by denying access and giving the illusion of risk for possible offenders (Prince William County Police Department). Another important feature in reduction of possible attacks is the physical design of the site. One would want to have features that define the property lines and distinguish between private and public areas. For an infrastructure such as the California ISO, there is a great need to protect the facility. Currently there is not a protection plan in place at the California ISO. The California ISO is left unprotected. With any major physical or cyber incident California could be without power for long periods of time.

In order to protect our critical infrastructures, there are many ideas that can be used with the natural lay of the land. The CPTED Strategies recommend a number of ways to do this for a facility such as the California ISO. The recommendations include lighting around the facility to ensure that visitors and employees can visibly see the site, positioning parking attendants should be done so that they have a clear visibility of the property, using walls wherever necessary and making sure they are high enough to

prevent circumvention. This also avoids creating hiding spots any place on the property. These are examples of the use of natural surveillance. There is also the use of natural access control which calls for avoiding dead-end driveways and streets allowing surveillance opportunities for patrol, securable site entrances, restricting access to roofs, keeping building entrances to a minimum and monitoring them, using a separate, well-marked, monitored entrance for deliveries, restricting access between different areas internally and externally, and providing access to both the front and back of the site so that the grounds can be patrolled. All of these help the infrastructure from possible attacks by using a monitoring and surveillance that is readily available to the site via patrol. It is also useful to create a "well defined entrance or gateway with planting, fences, gates, etc." (Prince William County Police Department, p. 18). It's important to separate employee parking from the visitor parking as well to ensure that patrols can distinguish newcomers and people that should not be on-site.

Economic impact

In 2001 California was suffering from an electricity crisis which had a major impact on the economy within California and those businesses depending on the electricity. There was a sharp increase in the wholesale electricity prices which reduce the growth for both businesses and household consumers. Due to the supply demand issue the California ISO estimated there would be somewhere in the area of 110 hours of possible rolling blackouts (AUS Consultants, 2001). With these rolling blackouts they estimated that there would be major undesirable implications for the growth of the state’s

economy and would result in lost jobs and a decline of income for those in California. The following is a number of the economic impacts, found by the AUS Consultants that reported on the situation in 2001, that California would face that year due to the rolling blackouts:

- Gross State Output for California would be reduced by $21.8 billion, or 1.7 percent in 2001. This would reduce the growth rate of California gross state output from the 2.3 percent currently projected. The loss has two components:
    - A direct loss of output experienced by all industries due to the effects of the blackouts in the amount of $6.8 billion. Of this, California's manufacturers would lose 18 percent, or more than $1.2 billion.
    - An indirect effect reflecting the fact that each dollar of output by one industry represents the purchase of output (i.e. goods and services) by other industries. This amounts to $14.9 billion.
- A loss of output of this magnitude would reduce household income for California by $4.6 billion. This is a loss of $104 for every one of California's 11.5 million households. Important to note is that this loss in addition to the impact of higher electricity costs.
- 135,755 jobs would be lost in all industries in the California economy.

Chapter 3

PROJECT PROCESS

The California ISO

The California ISO manages the flow of electricity across the high-voltage, long-distance power lines that make up the large majority of California's power grid. It is the ISO's job to ensure the "keeping of the lights on." The California ISO is the operator of the grid and a not-for-profit organization. It opens access to wholesale power markets designed to expand resources and lower prices. It grants equal access to 25,526 circuit miles of power lines. Every five minutes the California ISO forecasts the state's electricity demand, accounts for operating reserves and dispatches the lowest cost power plant unit to meet that demand while distributing space on the power lines.

The California ISO opened the northern and southern California control centers in 1998 during the time when the state restructured its wholesale electricity industry. The California ISO acts as a traffic controller; it routes electrons, maximizing the use of the transmission systems and its generation resources. It also performs the maintenance of the lines. It is the nerve center for the California power grid. It matches buyers and sellers of electricity and facilitates almost 30,000 market transactions every day to make sure there is enough power on hand to meet the demand. It provides a level playing field so all qualified companies get fair access to the grid.

They are responsible for serving nearly 30 million Californians and keeping tabs on more than 1,400 power plant units. As the impartial grid operator, the California ISO

has no financial interest in any of the market, and it ensures diverse resources have equal access to the network and markets used to fine-tune the flow of electricity. It is responsible for operating the high voltage grid for most of the state of California. They ensure that power can be lessened as intended without overloads or congestion. To ensure safe and reliable operation of the grid, the California ISO manages power line bottlenecks that could overload key components and stop the flow of electricity. As part of the balancing that the California ISO has to do, it puts megawatts on standby to make sure that blackouts do not occur.

The California ISO was created as a result of landmark legislation, Assembly bill 1890, and started operations in March of 1998. The primary mission of the California ISO has always been the safe and reliable operation of California's Bulk Electric Transmission system. One of the simplest ways of explaining what it does is to compare it to the aviation industry; the California ISO is like the air traffic controller of electricity. It does not own the power plants or transmission lines, is not responsible for establishing service paths and does not collect money directly from its customers – just like aviation air traffic controllers. However, just like air traffic controllers, the California ISO's operators have operational authority over the transmission operators. It operates the "grid" by balancing daily use against established forecast. Just like an air traffic controller, Transmission Dispatchers, as they are referred to, have a margin for error that is extremely tight. Even the smallest miscalculation can result in widespread cascading outages (Alvarez, 2010).

Before the establishment of the independent transmission operators, electricity was a matter of local concern and was regulated strictly at the state level. There wasn't technology available to move electricity over large distances, which is why power plants were required to be close to the customers. Once the technology was available, it provided the ability to move the electricity over hundreds of miles; plants could then be located at almost any location and there was no concern about the customer's location. This is when the beginning of competitive markets arose.

In 1992 the Independent System Operators (ISOs) and Regional Transmission Organizations (RTOs) were created, and this began the wholesale side of the electricity business. The ISO was created to manage the power grid and also make sure competitive generations flowed to customers. Since it would be unfair for air traffic controllers to represent one airline and profit from allowing that company's planes to go through before others, similarly the ISOs and RTOs operate on their own and manage the power grid (which they do not own), ensuring that electricity is delivered to the utilities and consumers in a reliable fashion and timely manner.

The California ISO improves grid reliability, optimizes use of the transmission system, lowers wholesale prices, improves power plant availability and reduces market barriers for clean energy resources and demand response providers. Collectively the ISOs and RTOs provide 2.20 million gigawatt-hours of electricity annually and oversee more than 270,000 miles of high voltage power lines. Without the California ISO, it would be difficult for this power to get around in a reliable and timely manner, because there

would be no "middle man." The ISO is in charge of making sure that the transportation of electricity on the "electron superhighway" is safe and reliable.

The California ISO grid control room controls more than 80 percent of the state's total electrical load and serves more than 30 million of its residents. Another one of the main functions of the ISO is to give transparent information about the state of the system and pricing. It is pertinent that this information is given in a timely and accurate fashion because it is the main piece of an effective and competitive marketplace. The ISO is important because it is used to balance the system and without it the movement of electricity would come to a halt.

It is difficult to answer the question of what would happen if the California ISO was attacked either physically or a cyber attack. It depends on a lot of different factors. Using the analogy of the Aviation Industry; merely attacking an air traffic tower would not automatically cause airplanes to fall from the sky. Just like airline pilots can and do take independent actions to ensure the safety of their passengers, utility companies, and power plant managers can take independent actions to maintain operations. However, if the California ISO were to be attacked when reserves are tight, demand is high and resources are scarce the likelihood of significant negative impact is high (Alvarez, 2010).

Electricity is the lifeline of our society. Our way of living would not be possible without the collection of electrons called kilowatts. Electricity is a unique commodity and cannot be stored, so it has to be created the instant before it is consumed. This makes for keeping the lights on in California an around the clock job. Everyday at all times of the day the California ISO is matching the demand for electricity with just the right

amount of power. The ISO is the impartial link between power plants and the utilities that provide electricity to customers. The California ISO acts as a clearinghouse for nearly 30,000 market transactions ever day and is the gatekeeper to power lines connecting California to neighboring states as well as to Canada and Mexico. This gate keeping is because of the fact that during the summer months about one-quarter of California's power comes from outside the state.

In an interview with the Manager of Physical Security, Hector Alvarez states:

If the California ISO ceased to exist the transmission system could operate for a brief period of time without the California ISO, just like planes can fly without a control operator giving instructions. However, it is not an efficient or reliable method of operation. Imagine aviation traffic at Denver International Airport without flight controllers.

Prior to the California ISO electricity was run by the individual utilities. They were in charge of the power and generation. The California Public Utilities Commission (CPUC) and the separate entities were more hands on before deregulation. When deregulation occurred most of these utilities sold everything off and relied on the California ISO to balance the supply and demand. If the California ISO ceased to exist the utilities would end up having to take over the supply and demand. There were specific requirements put in place so that the utilities are unable to communicate with one another on certain critical issues. They are then unable to test their processes for "what ifs" like if the California ISO did not exist (Thompson, 2010). So if it was brought down in an attack of some kind the utilities could pick up some of the process but a lot of it

would be chaos. Losing the this infrastructure would mean losing years of knowledge and industry specific education. There are not many people in the world that can do what we do here. The California ISO employs people that are specific to the electricity industry and what the it does and there is no other place that does this. There are other ISO facilities, however they function differently than the California location does and would not be able to jump in and begin piecing the California ISO back together. Most of the California ISO's policies and procedures lie on the premises and would be lost if the it was attacked (Thompson, 2010). The loss of the facility would mean a loss of coordination between power entities and therefore there would be possible blackouts around California and other Western states, including Mexico (Thompson, 2010). These blackouts could cascade into a larger possibility of potential chaos in places like Mexico because it is all electrically connected. The separate utilities do not see the same view that the California ISO does and so it makes it very difficult for them to know what is going on at all times with all the equipment.

The California ISO also runs the financial piece of the electricity. They make sure the markets are running and reliable. Without it there is no one to coordinate this piece and therefore it would fall off the radar. The settlements the California ISO runs with the entire money related piece would not be facilitated and the flow of money would halt. It runs a large number of systems within the facility that are pertinent to keeping the grid up, keeping everything reliable, and making sure electricity is getting to where it needs to go. One of the big concerns with the California ISO is an attack on our internal systems. A sabotage attack on a system could potentially cause a long term debilitating issue. If

the ISO is unable to monitor the systems because someone has hacked in there would be the possibility of markets going down, electricity not going to the correct spots, financial issues, equipment failing and much more. Sabotaging our systems could possibly last for a while before anyone was able to catch it because it is not an attack that everyone would see like an external attack. It would take time to see it, evaluate it, and then resolve it.

Keeping organizational assets protected in today's world is a challenge that becomes increasingly more difficult with new products and intruder tools. Most of the institutions recognize that it is not a single level of security that is needed out there but instead a multi-tiered security strategy. At Manitoba Hydro, a provincially owned power utility in Canada, they have become increasingly concerned with the possibility of a cyber attack on their systems that run and control the grid and the data that is within all these systems. "The vulnerability of these systems has gained attention in recent years as media reports have highlighted the potential threats posed by hackers breaking into these systems and remotely controlling or sabotaging the electric grid" (Johnson, McColm, & Powell, 2009, p.50). Addressing the threat from the inside and the outside requires a comprehensive, converged enterprise security plan with strong fundamentals, including strong procedures for ensuring personnel security and multiple factors of network access control that change regularly to prevent access by outsiders and or insiders (Johnson, McColm, & Powell, 2009, p.50). How does an institution go about preventing a cyber attack such as this? Network access control can be a simple solution with regular IT security awareness training, awareness programs, use of strong passwords, remote access authentication and encryption (Johnson, McColm, & Powell, 2009, p.50). In 2005, the

North American Electric Reliability Corporation (NERC) issued a number of standards that would prevent critical cyber attacks. Many of these utilities like the California ISO contain a number of logical and physical critical assets that control or manage the power grid. If someone were to gain access to these assets, the California ISO would be at a huge risk along with those entities that it works with.

Similarly, during the height of the energy crisis years ago hackers attacked one of the ISO computer systems that is an integral part of the movement of electricity throughout California. While the lapses in computer security have since been fixed and there was no imminent danger to the grid, the hackers still came very close to gaining access to key parts of the system, which could have then seriously disrupted the movement of electricity across the state. Many of the state lawmakers were angered by the breach at an entity like the California ISO, who is such a basic part of California's power system, given it is fragility during the state's energy crisis. This attack on the facility had the potential for more serious consequences; they were able to gain access into the headquarters in Folsom that links to a system that controls the flow of electricity across California. This state system is tied into the transmission grid for the western United States.

Had the hackers been able to get deeper into the system there was a possibility that it could have affected our reliability of our internal networks. The California ISO is an essential component of the state's electricity system. The purpose behind the California ISO is to balance the flow of electricity across the state and make last-minute power purchases to match demand and avoid blackouts. With the possibility of having

hackers gain access to our system means that there is a possibility that many Californians would lose power and there would be issues within the market. The electronic intrusion looked at in the light of September 11th, unnerves the California ISO.

The California ISO currently has a facility in Folsom, CA that is potentially unsecure and is a potential target for attacks (Alvarez, 2010). With the amount of destruction and damage that could be done with the loss of the facility, there is a great need to take the time and money to invest in making it a more secure facility. “The electricity manager is supposed to have a 150-foot buffer between its control room, and all roads, but that is impossible in its present location” (Lamb & Shaw, 2008). The California ISO is currently composed of three independent business buildings and has been criticized for its inadequate location for protection from possible saboteurs by numerous assessment teams.

Where the California ISO is currently located there is a need for better protection around all of the three business buildings. Perimeter security at the current location of the ISO is non-existent. Anyone can drive into the parking lot without being questioned and without being checked in. One can drive all the way around the side of the building and park their car within feet of the grid that runs the electricity for California and the Western States.

The perimeter security can influence who goes in and even who goes out. In order to ensure that the grid is safe, and that there is that 150-foot buffer, a strong perimeter is needed around the ISO in its entirety. The current location of the facility cannot clearly identify its perimeter because the buildings are so close to other public buildings that

have public access requirements. To have the ability to identify the perimeter would mean a fence surrounding the entire facility which is nearly impossible currently because some of the California ISO buildings are shared with other non California ISO companies. While the fence helps secure the building from the outsiders it is also important to have a camera system set up to ensure that all areas are visible to the security staff. It is important to have CCTV on the fence to make sure all blind spots are covered. The parking lot for the Folsom facility is open to anyone who wants to enter. There are numerous entries and exits surrounding the campuses and they make it difficult to track visitors or potential attackers. To protect the California ISO, there needs to be manned entry control points that allow officers to easily regulate authorized and unauthorized traffic. At the manned station(s) there should be an identification verification area or checkpoint, an area that is designed specifically for vehicle inspections if needed at a higher threat level. There needs to be an area where a vehicle can turnaround if denied entry or if the vehicle has made a wrong turn, and then there should be some sort of barrier or crash barrier that stops a vehicle that is intent on entering the facility. Simple additions like the ones listed make for a huge security impact, especially when threat levels increase. If the threat level increases there should be a plan around entry requirements and closing off certain areas to those individuals who are not authorized at the higher threat level. Currently, that cannot happen and no matter the threat level anyone and everyone can enter the site.

The California ISO currently has a relationship with local law enforcement agencies, however there is an opportunity for the California ISO to utilize these

relationships and involve them in tactical training around the facility. It is important that the law enforcement agencies that would be responding to an event at the site know the facility inside and out. This type of training would allow the agencies to respond in an effective and timely manner. It also allows the employees a chance to touch up their training during an incident. In regards to training, there is a great need to train employees on site at the California ISO. In the literature read, many speak to Antiterrorism training and awareness that should take place among facilities employees and those involved with that facility. This type of training gives employees a better understanding of how to protect the facility and how to protect themselves. It focuses on identifying potential attacks, preventing terrorists from collecting data on the site, and how to report any suspicious activity. The California ISO struggles currently with the reporting piece. Many of the employees on site do not know how to report these suspicious findings nor do they know who to report them to and so they go unreported. The California ISO needs to remember it is not just physical protection that is needed but also internal protection. This type of protection comes from up to date policies, procedures, and training.

The lighting as described earlier in the research is very important for a secure facility. The California ISO currently does not have a plan in place that mandates lighting inspections. Lighting around such a facility is important because it allows security officers the ability to make their rounds without disclosing their presence. Appropriate lighting also discourages possible intruders by revealing persons within the area. It currently needs a plan to conduct inspections during higher threat levels. There should

also be a plan in place that calls for lighting checks on a regular basis by employees and security officers. The employees need to know what they are looking for and who to notify. Currently the California ISO rents a space from a property owner and at times the California ISO management is unable to make changes to the lighting around all facilities because the landlord is unavailable. This makes securing the campus very difficult.

As noted earlier, many facilities are using the natural terrain to protect their building. As of now, the California ISO's current location does not have natural terrain to use. In that case it is recommended that boulders, rocks, dirt berms and landscaping be brought in to protect areas of the site that are more critical. There needs to be an adequate standoff and currently the California ISO does not have that. There are many avenues that can be taken in creating an adequate standoff. Large rocks or concrete pots are examples of how the it can create a more natural standoff area to protect the facility since they do not currently have a terrain that does so naturally. During higher threat levels there should be a plan to increase the barriers around the building. Currently the California ISO does not have a plan that speaks to the barriers and the plan to control traffic during these higher threat levels. What should occur during a higher threat level is more barriers should be moved into place to create more of a standoff for the facility. The Appendix gives some recommendations of other questions that should be asked to ensure a safe facility.

Not only is the outside of the California ISO not protected but the inside lacks controls as well. The current facility has a mailroom for shipping and receiving parcels that is not isolated and pulled away from high traffic areas. The current mailroom is open

to everyone and all delivery trucks can pull right up to the back of the building without prior inspection and without prior authorization. Currently the mailroom backs up to a number of employee offices and poses a possible threat if there was any suspicious material in the area. There is no place in the mailroom at this facility for screening and sorting. The mailroom needs to be located in an area that is pulled away from large numbers of employees and the staff within the mailroom need to have the knowledge on how to handle possible suspicious parcels. In the event that the mailroom personnel finds a suspicious parcel they need to be trained on how to respond and there needs to be containers that allow disposal if necessary. There is a need to assess the current evacuation route in the event that a suspicious package was found. Currently many employees would need to evacuate past the mailroom, which is ineffective. There should be an alternate route set up so that personnel do not have to evacuate past the mailroom. The California ISO facility needs to look at long and short-term fixes. In order to ensure that the facility is not attacked during times where it is very likely there needs to be plans in place and begin with quick fixes that resolve immediate dangers.

Chapter 4

RECOMMENDATIONS

Conclusions and Future Considerations

This project exposed the vulnerabilities that exist at the current site of the California ISO. The California ISO currently goes highly unguarded with little or no site security except for minimal guard protection and camera coverage. There are many opportunities in which the facility could improve their security with short or long term fixes. Some of the fixes resolve issues that have faced the California ISO only recently with the new threats, but many fixes would need to be long term and these would ensure the security of our power grid in a time of attack.

First, the California ISO's current facility has been looked at in depth because of the current security vulnerabilities that lie near the actual power grid. There is supposed to be a 150-foot buffer between the control room, and all roads, which currently is not the case at the California ISO. The California ISO currently has three building locations spread apart from one another and has been criticized for its inadequate location. Overall, the site security at the site is inadequate for what the California ISO does and what would be lost without this specific site.

The solution is straightforward. The California ISO needs to install bollards (short vertical posts) around the building where the grid is located which would then minimize the amount of access one has to get near the grid. The bollards provide an easy

way to restrict cars or large trucks from getting to close to the building, yet are not intrusive to the buildings scenery.

Second, the California ISO must begin putting a perimeter security plan in place. There are three main driveways into the campus of the facility. To protect the California ISO, there needs to be manned entry control points that allow officers to easily regulate authorized and unauthorized traffic. At the manned station(s) there should be an identification verification area or checkpoint, an area that is designed specifically for vehicle inspections if needed at a higher threat level. There needs to be an area where a vehicle can turnaround if denied entry or if the vehicle has made a wrong turn, and then there should be some sort of barrier or crash barrier that stops a vehicle that is intent on entering the facility.

Third, it is important that the law enforcement agencies that intend to respond to an event at the California ISO know the facility inside and out. This type of training would allow the agencies to respond in an effective and timely manner. It also allows the employees a chance to touch up their training during an incident. In regards to training, there is a great need to train employees on site at the facility. Simply put there needs to be a routine training program in place, which focuses on employees, and those actually working onsite. Training people on a regular basis reminds them of how to react in an emergency.

Fourth, there should be a plan in place at the facility that calls for lighting checks on a regular basis by employees on site and by officers that are on patrol or monitoring the cameras. Individuals need to know what they are looking for and then who to notify

when there is an issue. While it may seem small, lighting allows the campus to be monitored by the CCTV system at all times, night or day. Another simple fix to the solution is having an agreement with the property owner to allow us to make changes to the lighting at our own will. The California ISO needs to be responsible at all times for the lighting on the campus of their facility.

Fifth, it does not currently have a terrain to use to assist with its protection. There are many avenues that can be taken in creating an adequate standoff. Large rocks or concrete pots are examples of how the California ISO can create a more natural standoff area to protect the facility since they do not currently have a terrain that does so naturally. During higher threat levels there should be a plan to increase the barrier around the building.

The sixth and final solution goes to the controls that allow certain things in the California ISO from external resources. The mailroom needs to be located in an area that is pulled away from large numbers of employees and the staff within the mailroom need to have the knowledge on how to handle possible suspicious parcels. In the event that the mailroom personnel finds a suspicious parcel they need to be trained on how to respond and there needs to be containers that allow disposal if necessary. There is a need to assess the current evacuation route in the event that a suspicious package was found. Currently many employees would need to evacuate past the mailroom, which is ineffective. There should be an alternate route set up so that personnel do not have to evacuate past the mailroom.

Like many high risk companies, the California ISO faces many challenges. With these few things in place the facility would be better protected from external attacks and internal attacks. Currently, it does not change anything externally during a higher threat level. With these few fixes that have been discussed there is the ability to move things around during higher threat levels and begin to secure the building even more. These are recommendations that can easily be put in place and can give the current California ISO facility a much stronger perimeter security.

APPENDIX

Based on the foregoing information these are primary threats and responses, which are recommended to the California ISO. This checklist is a tool to be used to assess and understand the possible security threats to the physical site of the California ISO. This is a useful tool to assist in determining the security risk level at the site. With the recommendations listed below the California ISO site security could be greatly enhanced and would provide much better protection against a possible attack.

Public areas

1. Are parking areas clearly marked? (i.e. visitor, employee, security,& catering)
2. Are nighttime lighting levels adequate for the level of traffic in all areas of the building and parking lot?
3. Are parking areas fully lit during all hours that people are on the site?

Restricted Access Areas

1. Are barriers in place to prevent unauthorized vehicles and pedestrians to access restricted areas or any area that is on the site that they have not been authorized to visit? (i.e. fences, locked gates, badge entry, barricades)
2. Are resources at the site instructed to report unauthorized people in restricted areas and other suspicious people in general to onsite security?
3. Are there visible signs posted that state no unauthorized visitors?
4. Are public areas in the building clearly defined from private areas within the ISO?

Security

1. Are there security officers in areas where there are strong likelihoods that something may occur?

2. Is there a perimeter fence that prevents unauthorized individuals to obtain access to the site if not permitted?

3. Is there a guard kiosk at each perimeter access point?

4. At the guard kiosk is there an authentication method for individuals who are authorized to be on site? (i.e. a badge reader at the kiosk)

5. Is there CCTV? And does the area surrounding the facility have enough light that it does not block the surveillance?

6. Is there signage in the front or entry way of the building? If so it should be removed so that the site is not drawing attention.

7. Is there 24/7 site security patrol on the ISO site to ensure that the property is being inspected at all times that a resource is there?

8. Are there windows that would allow an outside to view into the control room of the ISO and obtain confidential information?

9. Is there access points to critical areas that have an additional verification (i.e. mantraps, security kiosk, revolving door)?

Outside agencies

1. Has training been conducted on a regular basis with the Folsom Police Department?

2. Has training been conducted with the Sacramento County Sheriff's Department, the bomb squad, SWAT, and California Highway Patrol?

3. Has a tactical site walk through with the local law enforcement and security on site at the California ISO taken place to determine areas that are vulnerable?

4. Has a relationship been built with all local law enforcement to ensure that they know how to respond to an event at the California ISO?

5. Is there a rooftop spotting creation- there should be a visible marking on the rooftop in the case that aircraft needs to find the California ISO in an emergency they would be able to spot it from the air without problems?

REFERENCES

Alvarez, H. (2010, April 02). Manager, Physical Security. (S. Brow, Interviewer)

Bella, R. (2010, March 25). Burglars steal, destroy Molalla water system computer . *The Oregonian.*

City of Scottsdale, Arizona. *Construction Site Security*. September 2006. Web. April 2010. <http://www.scottsdaleaz.gov/Assets/Public+Website/bldgresources/Construction+Site+Security.pdf >

Consultants, A. (2001). *Impact of a Continuing Electricity Crisis on the California Economy.* Moorestown: AUS Consultants.

Information Commissionder's Office: Guidence on Data Security Breach Management. March 2008. <http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/guidance_on_data_security_breach_management.pdf>

How to Prepare for a Terrorist Attack. (2010, February 03).

Johnson, R., McColm, C., & Powell, D. (2009). The Utility of Securing the Electric Supply. *Security Management* , 44-51.

Lamb, C., & Shaw, M. (2008). CA-ISO Plans $125M Facility. *Business Journal* .

Leung, Rebecca (writer). (2004). U.S. Plants: Open to Terrorists [Television Series]. MMIV, CBS Worldwide, Inc.

Moteff, J., & Parfomak, P. (2004). *Critical Infrastructure and Key Assets: Definition and Idenfication.* Congressional Research Services.

O'Connor, T. (2008, January 29). *Megalinks in Criminal Justice*: *Approaches to Target Hardening*. Retrieved April 05, 2010. <http://www.apsu.edu/oconnort/3440/3440lect06a.htm>

Prince William County Police Department. CPTED Strategies: Crime Prevention Through Environmental Design (n.d.). Retrieved April 05, 2010. <http://www.pwcgov.org/docLibrary/PDF/002035.pdf>

Richmond, J. Y., & Nesby-O'Dell, S. L. (2002). *Laboratory Security and Emergency Response Guidance for Laboratories Workng with Select Agents.* Office of Health and Safety.

Risk-Based Performance Standards Guidance. (2009) Washington: Department of Homeland Security.

Secure Community Network. General Target Hadening (2005). Retrieved March 28, 2010. http://www.snus.org/page.aspx?ID=104659

Thompson, M. (2010, March 31). Lead Business Continuity Planner. (S. Brow, Interviewer)

Zensinger, L. W. (n.d.). Protecting infrastructure against attack. *BE Magazine* , pp. 62-63.