GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Physical Security and Why It Is Important

GIAC (GSEC) Gold Certification

Author: David Hutter, icewalkerdave@yahoo.com
Advisor: Manuel Santander
Accepted: June 10th 2016

Abstract

Physical security is often a second thought when it comes to information security. Since physical security has technical and administrative elements, it is often overlooked because most organizations focus on "technology-oriented security countermeasures" (Harris, 2013) to prevent hacking attacks. Hacking into network systems is not the only way that sensitive information can be stolen or used against an organization. Physical security must be implemented correctly to prevent attackers from gaining physical access and take what they want. All the firewalls, cryptography and other security measures would be useless if that were to occur. The challenges of implementing physical security are much more problematic now than in previous decades. Laptops, USB drives, tablets, flash drives and smartphones all have the ability to store sensitive data that can be lost or stolen. Organizations have the daunting task of trying to safeguard data, equipment, people, facilities, systems, and company assets. The company could face civil or criminal penalties for negligence for not using proper security controls. The objective of physical security is to safeguard personnel, information, equipment, IT infrastructure, facilities and all other company assets. The strategies used to protect the organization's assets need to have a layered approach. It is harder for an attacker to reach their objective when multiple layers have to be bypassed to access a resource. The information in this paper will cover the importance of physical security along with the strategies that should be in place to implement physical security at facilities using administrative, technical and physical controls.

© 2016 The SANS Institute Author retains full rights.

1. Introduction

Physical security over past decades has become increasingly more difficult for organizations. Technology and computer environments now allow more compromises to occur due to increased vulnerabilities. USB hard drives, laptops, tablets and smartphones allow for information to be lost or stolen because of portability and mobile access. In the early days of computers, they were large mainframe computers only used by a few people and were secured in locked rooms (Harris, 2013). Today, desks are filled with desktop computers and mobile laptops that have access to company data from across the enterprise. Protecting data, networks and systems has become difficult to implement with mobile users able to take their computers out of the facilities. Fraud, vandalism, sabotage, accidents, and theft are increasing costs for organizations since the environments are becoming more "complex and dynamic" (Harris, 2013). Physical security becomes tougher to manage as technology increases with complexity, and more vulnerabilities are enabled.

Approximately 74,000 employees, suppliers, and contractors were affected by a data breach in 2014 because of stolen laptops with unencrypted personal data (Scott, 2014). In this case, the financial cost of the laptops was not the issue. A former employee filed a class action lawsuit against Coca-Cola claiming it was negligent in securing personal data. Environments now more than ever need to be concerned with "physical theft of devices and equipment" (Oriyano, 2014). Mobile devices including cell phones, laptops, and hard drives are easily portable, thus making them more susceptible to theft.

Theft of mobile devices is not the only way that attackers can get the data they want. An attacker could download sensitive data if he or she were to connect an external hard drive or flash drive to an unsecured computer. Leaving a USB flash drive on the ground outside of a building is another way that an attacker could steal data without ever gaining physical access. The malicious payload on the device infects an individual computer and possibly the entire network once an employee picks up the USB stick and inserts it into his or her computer. This type of incident happened at a U.S. Department of Defense base in the Middle East in 2008. An employee working at the base inserted a compromised USB memory stick into the government's laptop. The virus spread undetected in both unclassified and classified systems and sent data back to remote servers in other countries. (Lynn III, 2010).

David Hutter, icewalkerdave@yahoo.com

© 2016 The SANS Institute Author retains full rights.

The physical element of security is often overlooked. The theft of hardware or vandalism could occur while working with administrative and technical controls. Organizations often focus on technical and administrative controls and as a result, breaches may not be discovered right away (Oriyano, 2014). Information and have different weaknesses, risks, and countermeasures than physical security. When people look at information security, they conspire how a person may penetrate the network using unauthorized means through wireless, software exploits or open ports. Security professionals with physical security in mind are concerned about the physical entrance of a building or environment and what damages that person may cause.

Examples of threats that physical security protects against are unauthorized access into areas and theft of mobile devices. Attackers can gain entry into secured areas through tailgating, hacking into access control smart cards or breaking in through doors. Defenses for these threats include physical intrusion detection systems, alarm systems, and man traps. Mobile devices such as laptops, USB drives and tablets are easy targets because of portability. Control examples that could help stop theft are the use of RFID systems and cable locks.

"Physical security protects people, data, equipment, systems, facilities and company assets" (Harris, 2013). Methods that physical security protects these assets is through "site design and layout, environmental components, emergency response readiness, training, access control, intrusion detection, and power and fire protection" (Harris, 2013). Business continuity or disaster recovery plans are required to reduce business interruption in times of natural disaster, explosion or sabotage.

One security professional cannot cover the entire spectrum of physical security. Professionals that work in this space do not always have a holistic understanding of physical security because of specialized variables and components that are needed to secure an organization. Individuals often "specialize in specific fields, such as secure facility construction, risk assessment and analysis, secure data center implementation, fire protection, intrusion detection systems (IDSs), closed-circuit television (CCTV) implementation, personnel emergency response, training, legal, and regulatory aspects of physical security, and so on". (Harris, 2013).

Since physical security is usually further down the list of priorities, physical environments and facilities are not typically designed with security in mind. Aesthetics and

© 2016 The SANS Institute Author retains full rights.

functionality often take precedence over security concerns (Harris, 2013). If organizations focused on security in a holistic, organized and mature way, risks or causalities could be minimized Organizations can be held monetarily and criminally liable for not practicing due diligence. Examples of lawsuits that organizations can be held accountable include a unsecured laptop left by an employee containing PII was stolen and a company did not follow fire codes and death resulted because people could not escape through a locked exit door.

Physical security teams must implement a security program that balances security measures and safety concerns (Harris, 2013). Physical security should always use what is called a "defense in depth" (Oriyano, 2014) approach to reinforce security through different controls. Multiple security controls in places make it tougher for attackers to get to valuable company resources.

Security needs to increase the productivity in the environment by protecting assets. Good security practices in place allow employees to feel safe so they can focus on their tasks, and force attackers to pray on easier targets (Harris, 2014). We should think about how physical security can affect our organization using the CIA triad – confidentiality, integrity, and availability. We look at the areas of security that can affect the confidentiality of data, the integrity of assets and the availability of company resources (Harris, 2014).

Physical security must plan how to protect employee lives and facilities. The first priority of physical security is to ensure that all personnel is safe. The second is to secure company assets and restore IT operations if a natural disaster happens.

In the event of an explosion or fire, the right suppression methods must be utilized to contain the event. Using the wrong suppression agent can not only make the situation worse but also hurt people. There multiple types of suppressions that can be used to contain fires. Water, gases, and powders are used in different scenarios to extinguish one of the four fire elements: heat, oxygen, fuel, chemical reaction.

2. Planning For a Physical Security Program

Adequate controls are not present to control the physical environment without a plan in place. The company must create a team that is responsible for designing a physical security

© 2016 The SANS Institute Author retains full rights.

program when planning for security. The physical security team should continually improve the program using the defense in depth method.

Defense in depth is a concept used to secure assets and protect life through multiple layers of security. If an attacker compromises one layer, he will still have to penetrate the additional layers to obtain an asset. To give an example of this concept, let us say that you have a computer that an attacker wants to access. The computer in located inside a locked room within a building. The building has an access control system in place, and there is a fence with a guard outside. If the adversary only needed to climb the fence to get to the data, only one level of security is in place to stop an intruder. If we added security guards, access control systems, locked doors, this would make the task more difficult for the person trying to acquire a resource. In addition, logging into the computers and servers should require a smart card or token in addition to a pin or password in order to access proprietary data. These security measures working together provides multiple levels of security. To ensure that the security controls are working effectively, metrics should be used.

The team needs to identify key performance indicators (KPIs) to enhance the security program (Santander Peláez, 2010) KPIs should be monitored by period, quarter, current year, and over years (Wailgum, 2005). Metrics depend on the industry and organization. KPIs vary between corporations because of requirements and focus the organization has

Organizations need to use a “performance-based approach” (Harris, 2013) when measuring the physical security program. These metrics gauge how well the program is operating towards achieving the organization’s objectives. Data can be used to make informed decisions to lower risk in the most cost-effective method. Without these metrics, the security program will not be able to effectively manage security controls.

The following are key performance indicators to measure the effectiveness of the security program:

© 2016 The SANS Institute Author retains full rights.

Number of Successful Crimes
Number of successful crimes
Number of unsuccessful disruptions
Number of successful disruptions
Time between detection, assessment and recovery steps
Business impact of disruptions
Number of false-positive detection alerts
Time to restore operational environment
Financial loss of a successful crime
Financial loss of a successful disruption

(Harris, 2013)

Once key performance indicators are tracked, they can confirm the right objectives are being met. Metrics identify acceptable levels of risk for the organization through the use of input and output process measures. As an example, input process measures could include asset inventory and resource requirements. Outputs could include security assessments completed versus planned, and countermeasures deployed. These inputs and outputs when combined in this example, illustrates the facility asset inventory is secured.

Organizations are required to abide by federal laws and regulations. Agencies that govern these laws and regulations include the Federal Information Security Management Act (FISMA) 2.0, which states that government agencies should "continuously monitor" information that is security related. The 20CSC guidelines created by the National Security Agency (NSA), U.S. Department of Energy nuclear energy and other groups, indicate the top 20 critical security controls organizations can use to strengthen the security program. Agencies including the International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), Department of Homeland Security (DHS), Government Accountability Office (GAO) dictate how a company must comply, and threat modeling is a process that points out what could happen if a vulnerability is exploited. Together they make up the acceptable risk level for the company. The program should utilize the right balance of resources for each of the objectives so that they are not under or over allocated compared to the organization's threat profile.

David Hutter, icewalkerdave@yahoo.com

© 2016 The SANS Institute Author retains full rights.

The organization can verify if resources are allocated correctly through consistent monitoring of metrics. For an example, six security guards work during off hours. Four guards work from 4 P.M. until 1 A.M. The other two work from 1 A.M. until 9 A.M. and at all times at least one guard is required to be at the front gate. A report containing intrusion detection data, such as when and where alarm faults occurred, break-ins and theft at the warehouse occurred from 1:34 until 4:13 A.M was discovered while reviewing this report. The countermeasure of placing a guard from the afternoon shift at the warehouse during the early morning shift was initiated. Two months later, a report concluded that the break-ins at the warehouse went down 95%. As a result, the organization had a lower amount of break-ins and theft when resources were properly allocated. Utilizing metrics can be impactful to the company because it can show if the organization is making the right decisions.

The organization's threat profile depends on the nature of the business. It decides what types and levels of risks it should accept, transfer, avoid or mitigate. A threat profile includes targets, threats, threat agents, threat scenarios and vulnerabilities. The organization must have a clear understanding of how all the threat components work together to create a threat profile (Irwin, 2014). After risks are assessed, the team can go after priority items. The relationships of risks, baselines, and countermeasures that an organization can apply to define acceptable risk levels used in the threat modeling process can be seen in this example:

© 2016 The SANS Institute Author retains full rights.

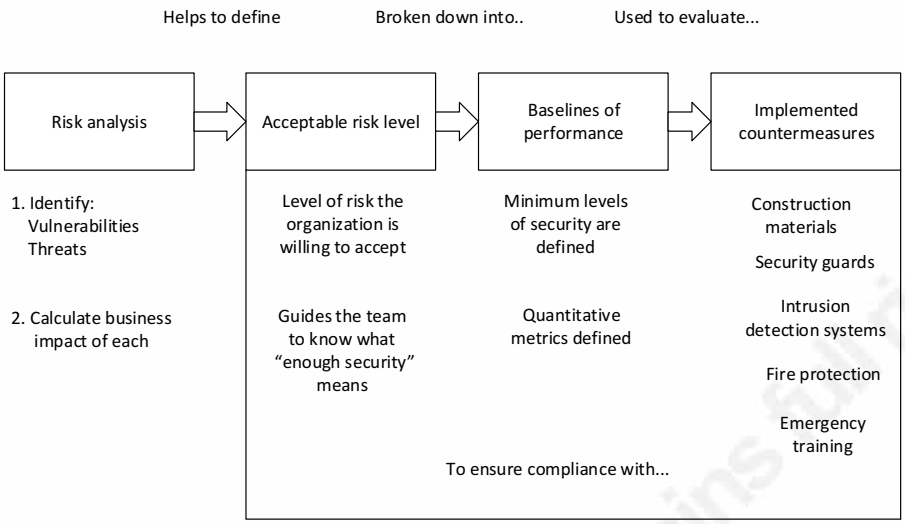


Figure 1 - Relationship of Risk...

Criminals should have to go through multiple layers of security to gain access to an asset. Businesses need to try to minimize incidents from occurring, and if they do, steps need to be in place to deal with them. Incidents must be detected. It is impossible prevent every intrusion, but all must be detected to minimize impact to the organization. Metrics from incidents including the cost of replacement, business impact, where, what time and what frequency did breaches occur, should be used to analyze what types of disruptions are impacting business operations.

Baselines are minimum security requirements that utilize metrics for program monitoring. When countermeasures are meeting the established baseline, the physical security program is successful and implemented effectively. Physical security baselines examples include: commercial or industrial locks are required in private areas, bollards (concrete pillars that block vehicles from driving into buildings) must be used in front of all public entrances, and door delay controls are mandatory on server room doors.

Physical security threats can be internal or external. Employees are considered internal threats and can utilize their knowledge of building layouts and where assets are located to steal or vandalize assets. Employees have the ability to gain access to areas unobserved because of

© 2016 The SANS Institute Author retains full rights.

their job duties. Predicting attacks from insiders it difficult to detect because their access permissions. Fire, water, and environmental failures are also internal threats.

An example of insider threat could be a security guard working off hours with access into all areas decides to commit crimes without alarming other employees. Employees should have background checks conducted when hired to protect company assets. Government agencies and organizations that work with them have access to classified data. Jobs in this space may require polygraph tests in addition to the background clearance.

Collusion is a type of insider threat that involves two or more employees. What is difficult about this risk is it can bypass procedural processes. Because of the nature of the specific job roles, employment screenings, rotation and separation of duties require more than one employee.

Natural disasters are considered external threats. External threats also possibly have a human factor such as protests, riots or bank robbers. These threats are primarily any outside force or person that does not have company ties.

The following tasks must be completed before a physical security program can be implemented:

Conduct risk assessments to identify threats and weaknesses. Next, conduct a business Impact analysis of all threats.
Work with the legal department to ensure that the organization is meeting and maintaining law requirements.
Have management set an acceptable risk level for the security program.
Calculate baselines after the risk levels have been established.
Use performance metrics to track countermeasures.
Outline performance requirements and levels of protection from analysis results from: Deterrence Delaying Detection Assessment Response
Implement and identify these countermeasures for all program categories.
Countermeasures must be evaluated regularly against baselines assuring that acceptable risk levels are not being surpassed.

(Harris, 2003)

3. Physical Security Controls

Physical security manages and protects resources in the form of administrative, technical and physical controls. Access control systems, intrusion detection systems, and auditing systems

© 2016 The SANS Institute Author retains full rights.

are examples of technical controls. Some examples of administrative controls are site location, facility design, building construction, emergency response and employee controls. Physical control examples include types of building materials, perimeter security including fencing and locks and guards.

Deterrence, denial, detection then delay are the controls used for securing the environment. Attempts to obtain physical resources should be deterred through the use of fences, gates and guards around the perimeter. Locked doors and vaults protecting physical assets through denial. Physical Intrusion detection systems (IDS) and alarms are the next lines of defense and notify first responders if a breach is detected. If attackers reach their target, security measures such as a cable lock on a computer must delay the suspect from acquiring assets until guards or police arrive.

3.1. Administrative Controls

3.1.1. Site and Facility Considerations

All sites should have automated controls in place to protect the physical environment. The first line of defense must be administrative, technical and physical controls. The last line of defense should always be employees. Limiting human interaction with attackers reduces the risk of injury. These controls must be at the center when applying and sustaining physical security to protect people, IT infrastructure and operations (Stewart, J., Chapple, M., & Gibson, D. 2012). Controls must be utilized so that attackers have an opposition to stop or delay them.

3.1.2. Facility Plan

The facility plan uses critical path analysis which is a systematic approach that identifies relationships between processes, operations, and applications. An example could be a company web server that needs access to the internet, power, climate control, computer hardware, storage location. In this example, resources that require securing are identified. Additionally, dependencies and interactions that support the business functionality are reduced to only the mandatory ones because the processes, operations, and applications were identified. Critical path analysis is the first stage securing the IT infrastructure. IT infrastructure includes computers, servers, networking equipment, water, electricity, climate control, and buildings. Pictured below as an example of a plan to ensure that all government facilities are ISC compliant within 36 months:

© 2016 The SANS Institute Author retains full rights.

Mission: Secure Facilities	**Goal:** Ensure all [agency] facilities are ISC compliant within 36 months.	
Objectives	**Actions**	**Results**
1. Assess all 100 [agency] facilities for compliance within 18 months	1. Complete all scheduled risk assessments on time (quarterly schedule) 2. Obtain consensus/ approval on recommended corrective measures (CMs) within 45 days of risk assessment	100% of risk assessments completed on time. 18 compliant facilities 90% of recommended CMs approved within 45 days (Remaining 10% approved within 60 days.)
2. Implement corrective measures as needed within 18 months of last assessment	1. Identify priority CMs, and coordinate as appropriate with facility managers 2. Award ID/IQ contract(s) for CM installation 3. Conduct post deployment 4. ISC compliance inspection	250 CMs identified as needed to make facilities ISC compliant Five ID/IQ contracts awarded to install 250 CMs in 82 facilities within 18 months of last risk assessment All CMs installed and validated

(DHS & ISC, 2009)

Using current and future technologies, such as operating systems or mobile devices simultaneously is important. Current solutions improve, and new ones emerge as technologies involve. It is necessary to strategize how the older legacy systems and the new systems will merge together. The integration of old and new systems is called technology convergence. An organization could potentially have multiple systems doing the same function as technologies change, creating inefficiencies and risk to the company as it can be difficult to differentiate which system performs a particular task. In some cases, such as an e-commerce website, multiple servers are required to run in parallel, so there is not a single point of failure. Another example could be the intrusion alarm system, fax, and phone line utilizing a single phone line cable. One phone line that different systems connects to is single point of failure and if an attacker compromised the line at one location, none of these systems would work. Having separate phone lines ran to each system would lower the risk of all three losing their connection at the same time.

Parties including management, employees, and especially safety and security personnel, should contribute to the site plan. Management should be in the planning process so they can make sure funds are available for the project. Employee safety concerns should be addressed during the creation of the facility plan. Security staff can point out important aspects of physical

© 2016 The SANS Institute Author retains full rights.

security. Security goals for the business and the facility are supported further when their knowledge is used to help make the site plan.

3.1.3. Site location

Geographical location, price, and size are factors that involve thought when purchasing a site location. Security requirements should always be the primary concern when determining a location. Buying an existing facility or building a new one also needs to be considered.

Site physical security involves deliberation of situational awareness. It is important to take into account that looting, riots, vandalism, and break-ins can occur (Stewart, J., Chapple, M., & Gibson, D., 2012). Other things to consider before determining a site is visibility, including the terrain around the building, facility markings, signs, neighbors, and area population. Accessibility to the site is important. Road access, traffic, and distance to train stations, freeways and airports are important aspects. Building facilities susceptible to these accounts should be avoided. Geographical areas prevalent to natural disasters are not ideal site locations. These threats cannot be avoided because natural disasters are not predictable. The IT staff, emergency personnel, management and disaster recovery team must be prepared and equipped to handle natural disasters. Disaster recovery plans contained within the business continuity plan is the overarching plan that list the details necessary to recover from a tragedy.

3.1.4. Facility Design

Before constructing a site, building, IT infrastructure, system, or other items, security requirements must to be understood. Some security issues that need mitigation planning include unauthorized entry, emergency evacuation, entry and exit direction, alarm usage and conductivity. The construction materials and methods used to construct the facility have to meet or exceed building codes and safety measures.

Wall design has to adhere to the minimum fire ratings required in different areas. The type of combustible material that is used and reinforcement for security obligations, such as protecting server rooms or areas that have critical IT equipment must met code standards. The same design principals apply to doors, plus door design looks at placement, how doors withstand forced entry, will it be monitored by the alarm system, hinge durability, door opening direction, locks needed, and glass requirements.

© 2016 The SANS Institute Author retains full rights.

Ceiling design takes into account the combustible material used, fire rating and weight. Drop-ceilings call for special considerations. For example, one wall separates an attacker from his target. The ceiling in both rooms is a drop-ceiling type and the wall does not extend far past the tiles. The attacker only needs to climb over the wall to achieve his objective.

Window design selects if windows should be alarmed, clear or frosted, shatterproof. The design also takes into account if adversaries could gain access through them.

Flooring design plans for the type of combustible material to use, weight the flooring can handle, burn through time, and standard or raised flooring. In a raised floor environment, accessible space under the flooring is primarily used for the addition of electrical or communications wiring.

Heating, ventilation and air conditioning (HVAC) design details placement of central system and vents, switches and values that can be shut off in emergency situations, if protected intake vents are needed, and positive air pressure.

The design of electrical systems includes consistent clean and voltage regulated power, dedicated feeders to provide large amounts of electricity if necessary, the location of electrical main and sub-panels, and alternate power sources.

Fire suppression and detection system design dictates the type of detectors, sensors and their locations, storage of suppression system when testing is conducted, and types of gases or liquids used in the system.

Gas and water design decides locations of shutoff valves, placement of underground water pipes and gas lines, and positive flow.

3.1.5. Environmental Crime Prevention

Crime prevention through environmental design (CPTED) attempts to reduce crime utilizing facility construction, environmental elements, and procedures to modify human behavior. This design model has improved due to necessity because crime types and surroundings have evolved. For example, now malicious people can pretend to be talking on their cell phone while conducting video reconnaissance. Attackers can hack into wireless networks and create denial of service attacks. CPTED is used in developing of neighborhoods, cities, and physical security programs. Landscaping, lighting, road placement, entrances, site

© 2016 The SANS Institute Author retains full rights.

layouts, and traffic circulation patterns are all tackled by CPTED (Harris, 2013). Behaviors modified with CPTED may be modified for the good or bad and elements that reduce crime also could make people fear crime.

An example of CPTED is mission critical servers located near an exterior wall should be moved in case of external force to the middle of the building where there is less chance of impact. Another instance is surveillance cameras should be placed in plain sight. If adversaries know they are being monitored, they may move to another target. Employees feel safer knowing that there is less chance of an incident.

Target hardening focuses on crime prevention also. It differs from CPTED in that it uses alarms, gates, locks, fences, and similar concepts to deny access through artificial and physical barriers. When using target hardening, the view of the environment is less appealing.

3.1.6. Securing Data

Data centers and server rooms that house IT or communications equipment must be off-limits to unauthorized individuals. These rooms have to be locked down to prevent attacks. These rooms should be protected and have limited access to those employees that require access for job duties. The more human-incompatible these rooms are, the less likely attacks are executed. Oxygen displacement, extremely dim lighting, cold temperatures and hard to maneuver due to little space, are methods used in creating a human inhospitable environment. These data center rooms store mission critical equipment and should be located in the middle of the facility and not in the basement, ground or top floors.

3.2. Physical Controls

Facilities need physical access controls in place that control, monitor and manage access. Categorizing building sections should be restricted, private or public. Different access control levels are needed to restrict zones that each employee may enter depending on their role. Many mechanisms exist that enable control and isolation access privileges at facilities. These mechanisms are intended to discourage and detect access from unauthorized individuals.

3.2.1. Perimeter Security

Mantraps, gates, fences and turnstiles are used outside of the facility to create an additional layer of security before accessing the building. Fences distinguish clear boundaries

© 2016 The SANS Institute Author retains full rights.

between protected and public areas. Materials used to create fences vary in types and strength. Protected assets dictate the necessary security levels of the fences. Types of fences include electrically charged, barbed wire, heat, motion or laser detection, concrete, and painted stripes on the ground (Stewart, J., Chapple, M., & Gibson, D., 2012).

Gates are entry and exit points through a fence. To be an effective deterrent, gates must offer the same level of protection equal to the fence; otherwise, malicious people have the opportunity to circumvent the fence and use the gate as the point of intrusion. Construction of gates should consist of hardened hinges, locking mechanisms, and closing devices. Gates should be limited in number to consolidate resources needed to secure them. Dogs or surveillance cameras should monitor gates when guards are not present.

Turnstiles are a type of gate that allows only one person to enter. They must provide the same protection level as the fence they are connected. Turnstiles operate by rotating in one direction like a revolving door and allow one individual to leave or enter the premises at a time.

Mantraps are small rooms that prevent individuals from tailgating. The design of mantraps only allows one person may enter at a time. The idea is to trap the person trying to gain access by locking them inside until proof of identity is confirmed. If the individual has permission to enter, the inside door opens allowing entry. This is a security control measure that delays unauthorized people to entering the facility until security or police officers arrive.

3.2.2. Badges

Proof of identity is necessary for verifying if a person is an employee or visitor. These cards come in the forms of name tags, badges and identification (ID) cards. Badges can also be smart cards that integrate with access control systems. Pictures, RFID tags, magnetic strips, computer chips and employee information are frequently included to help security validate the employee.

3.2.3. Motion Detectors

Motion detectors offer different technology options depending on necessity. They are used as intrusion detection devices and work in combination with alarm systems. Infrared motion detectors observe changes in infrared light patterns. Heat-based motion detectors sense changes in heat levels. Wave pattern motion detectors use ultrasonic or microwave frequencies that

© 2016 The SANS Institute Author retains full rights.

monitor changes in reflected patterns. Capacitance motion detectors monitor for changes in electrical or magnetic fields. Photoelectric motion detectors look for changes in light and are used in rooms that have little to no light. Passive audio motion detectors listen for unusual sounds.

3.2.4. Intrusion Alarms

Alarms monitor various sensors and detectors. These devices are door and window contacts, glass break detectors, motion detectors, water sensors, and so on. Status changes in the devices trigger the alarm. In hardwired systems, alarms notice the changes in status by device by creating a wiring short. Types of alarms are deterrent, repellant, and notification.

Deterrent alarms attempt to make it more difficult for attackers to get to major resources by closing doors and activating locks.

Repellant alarms utilize loud sirens and bright lights in the attempt to force attackers off the site.

Notification alarms send alarm signals through dial-up modems, internet access or GSM (cellular) means. The siren output may be silenced or audible depending on if the organization is trying to catch criminals in the act.

3.3. Technical Controls

The main focus of technical controls is access control because it is one of the most compromised areas of security (Harris, 2013). Smart cards are a technical control that can allow physical access into a building or secured room and securely log in to company networks and computers. Multiple layers of defense are needed for overlap to protect from attackers gaining direct access to company resources. Intrusion detection systems are technical controls that are essential because they detect an intrusion. Detection is a must because it notifies the security event. Awareness of the event allows the organization to respond and contain the incident. Audit trails and access logs must be continually monitored. They enable the organization to locate where breaches are occurring and how often. This information helps the security team reduce vulnerabilities.

© 2016 The SANS Institute Author retains full rights.

3.3.1. Smart Cards

Token cards have microchips and integrated circuits built into the cards that process data. Microchips and integrated circuits enable the smart card to do two-factor authentication. This authentication control helps keeps unauthorized attackers or employees from accessing rooms they are not permitted to enter. Employee information is saved on the chip to help identify and authenticate the person. Two-factor authentication also protects computers, servers and data centers from unauthorized individuals. Assess will not be granted with possession of the card alone. A form of biometrics (something you are) or a PIN or password (something you know) must be entered to unlock the card to authenticate the user.

Access token smart cards come in two types, contact and contactless. Contact smart cards have a contact point on the front of the card for data transfer. When the card is inserted, fingers from the device make a connection with chip contact points. The connection to the chip powers it and enables communication with the host device. Contactless smart cards use an antenna that communicates with electromagnetic waves. The electromagnetic signal provides power for the smart card and communicates with the card readers.

Access token cards are thought to be impervious to tampering methods; however, these cards are not hacker proof. Security is provided through the complexity of the smart token. The smart token only allows the card to be read after the correct PIN is entered. Encryption methods keep malicious people from acquiring the data stored in the microchips. Smart cards also have the ability to delete data stored on it the card detects tampering.

Cost is a disadvantage of smart card technology. It is expensive to create smart cards and purchase card readers. Smart cards are basically small computers and carry the same risks. As technology evolves, storage capacity and the ability to separate "security-critical computations" (Harris, 2013) inside the smart cards. Smart cards can store keys used with encryption systems which helps security. The self-contained circuits and storage, permit the card to use encryption algorithms. The encryption algorithms allow for protected authorization that can be applied enterprise-wide.

David Hutter, icewalkerdave@yahoo.com

© 2016 The SANS Institute Author retains full rights.

3.3.2. Smart card Vulnerabilities

Malicious individuals are encouraged to steal valuable information that can be compromised. Attackers attempt to bypass smart card vulnerabilities by various methods including fault generation, side-channel attacks, software attacks and microprobing.

Fault generation involves trying to reverse-engineer smart card encryption. The goal is to locate the encryption key so that they information stored on the smart card can be accessed. Fault generation consists of entering computational errors into the card by changing temperature fluctuations, clock rate and the input voltage (Harris, 2013).

Side-channel attacks expose data about how the smart card works without cracking it. The attacker observes how the device reacts to diverse situations making it a stealthier approach to uncover data. The attacker gathers information about the card through timing, differential power analysis, and electromagnetic analysis. Timing verifies the duration that the process takes to finish. Differential power analysis tests the processing power emissions. Electromagnetic analysis tests the release of frequencies. Attackers can use this information together to surmise the data stored on the smart card.

Software and side-channel attacks are considered noninvasive attacks. Smart cards are microprocessor devices and contain software located on the chip that processes data. The software can be hacked because it has vulnerabilities that can be compromised. Software attacks load commands that permit the adversary to excerpt account data. An attacker could purchase items illegally if the account information is extracted from the card. The appearance of the devices used to conduct software and side-channel attacks appear to be average equipment.

Microprobing is a more intrusive attack because it involves connecting probes to the access token card microchip and interacting directly with it the internal parts. The objective of microprobing is to remove the chip from the card. The first step is to use microprobing to remove the protective top layer contact cards using ultrasonic vibration. The EEPROM chip can be set or reset or modify any bits in ROM chips using two needles once the passivation layer is removed, (Boudriga, 2009).

David Hutter, icewalkerdave@yahoo.com

© 2016 The SANS Institute Author retains full rights.

3.3.3. Proximity Readers and RFID

Access control systems use proximity readers to scan cards and determines if it has authorized access to enter the facility or area. Access control systems evaluate the permissions stored within the chip sent via radio frequency identification RFID. This technology utilizes the use of transmitters (for sending) and responders (for receiving).

In physical access control, the use of proximity readers and access control cards that contain passive tags are used. Passive tags are powered from the proximity readers through an electromagnetic field generated by the card reader. A signal is sent to the reader when a card is swiped. The door unlocks once the signal is received and verified.

Active tags contain batteries to self-power the RFID tag. Active tags have a battery power source built in that allows them to transmit signals further than passive tags. However, the cost of these are significantly higher, and their life is limited because of battery life. These are typically used to track high-value items. Readers can track movements and locate items when connected to the network and detection systems. If an asset is removed from certain areas, the organization can have the access control system trigger an alarm.

3.3.4. Intrusion Detection, Guards and CCTV

If the equipment is relocated without approval, intrusion detection systems (IDSs) can monitor and notify of unauthorized entries. IDSs are essential to security because the systems can send a warning if a specific event occurs or if access was attempted at an unusual time.

Guards are a significant part of an intrusion detection system because they are more adaptable than other security aspects. Security officers may be fixed at one location or make rounds patrolling the campus. While making rounds, guards can verify doors and windows are locked, and vaults are protected. Guards may be accountable for watching IDSs and CCTVs and can react to suspicious activity. They can call for backup or local police to help capture a suspect if necessary.

Closed-circuit television or surveillance systems utilize cameras and recording equipment to provide visual protection. In areas that cameras monitor, having enough light in the right areas is essential. It might be too dim for the camera to capture decent video quality necessary to prosecute or identify persons of interest without enough light. Cameras can be fixed lens (not

© 2016 The SANS Institute Author retains full rights.

movable) or zoom lens (adjustable). In monitoring something that is stationary, you would want to use the right type of fixed lens depending on distance and width you are monitoring. Fixed lenses are available in wide, narrow or wide-angle. Zoom lens are recommended when viewing a target that might need an enlarged view. Another type of camera is a pan, tilt, zoom camera. These are dome style cameras that have the ability to move in all directions as well as zoom in. PTZ cameras are best for tracking suspects because the camera automatically detects and follows a suspect. PTZ cameras can auto track moving objects through mechanical or application methods. Cameras that use software applications have the ability to change targets and can filter out images that are stationary, saving bandwidth and storage.

Digital video recorders (DVRs) are used to support cameras. They store what the camera views and can replay break-in video or for evidence. DVRs includes software that allows for manual PTZ control, which cameras are zoomed in on. They also have a multiplexor built in so they can record multiple camera feeds simultaneously. Cameras stream video data through coax, wireless or IP means. Some DVR systems allow for a user to incorporate them into their network for additional storage capacity or remote viewing purposes. IP cameras can also connect to computer based DVR systems that have software installed on the host machine. These computers have more functionality and storage capacity than DVRs and require it because IP cameras need more storage space because of the higher definition video.

3.3.5. Auditing Physical Access

Auditing physical access control systems require the use logs and audit trails to surmise where and when a person gained false entry into the facility or attempted to break-in. The software and auditing tools are detective, not preventive. Consistent monitoring of audit trails and access logs are needed to act swiftly. The system has no value if the organization does not respond or response time is limited. Management needs to know when there are incidents so they can make security decisions. Adding additional resources to particular areas or at certain times might be necessary to protect the environment. Access logs and audit trails must include the date and time that the incident occurred. These logs should capture all failed access attempts, the person's employee information, and location where the attacker tried to gain entry.

© 2016 The SANS Institute Author retains full rights.

4. Life and Environmental Safety

The most important physical security is protecting human life. Physical security must always be taken seriously in facilities. Preventing injuries to employees and protecting basic environmental elements at site location should be the first priority in a physical security program.

4.1. Employee Safety and Privacy

The basic environmental essentials should be preserved to maintain employee safety. Human life threats and the stability of the site can be the direct result of natural disasters, release of toxic materials, flooding or fires. The physical security actions team should have procedures in place to safeguard against these types of events. The first action required is to focus on human safety. Second, the restoring of utilities necessary for IT operations can take place after all safety measures are met. In extreme cases such as natural disasters, guidelines and plans must be in place to properly deal with the situation.

Occupant emergency plans (OEP) are guides that assist with sustainment of employee safety after a natural disaster occurs. It outlines how to diminish human life threats, avoid injuries, conduct travel arrangements, ways to monitor safety, cope with duress, and defend property destruction if a damaging physical incident were to impact the site. OEP only addresses staff and limited property damage. Business continuity planning (BCP) and Disaster recovery planning (DRP) address business and IT functionality.

4.2. Power and Electricity

Electricity requirements are necessary so that electronic equipment can function correctly. Organizations need specialized equipment help to cope with issues like dirty, inconsistent power. “Dirty power” is a term that refers to electricity having noise, voltage irregularities and frequency anomalies. An Uninterruptible power supply (UPS) system is used to manage these matters. UPS systems take electricity in and store it using batteries. The system then outputs clean and regulated electricity that is essential for electronic equipment. With the power stored inside batteries allows the electronic system to function in the event of a power outage. UPS systems provide electricity for a limited amount of time, but it can allow for the proper shutdown of IT systems if necessary. Electronic equipment also becomes damaged from voltage irregularities. Voltage regulators keep voltages consistent, and the use of surge protectors

© 2016 The SANS Institute Author retains full rights.

should be utilized to protect against high voltage incidents. In the event of losing electricity, backup generators can provide electricity to restore business functions if required.

4.2.1. Noise

Noise can affect the quality of any data transmission systems that utilizes electromagnetic transport means. Electromagnetic interference and radio frequency interference can cause disruption to communication systems such as cellular, computer network, phone, auditory, radio, television, etcetera (Stewart, J., Chapple, M., & Gibson, D. (2012). Noise is caused by arching equipment, solid-state rectifiers with loads, improper grounding, control devices, arching equipment, and power supply switching (CEDIA, 2008)

Electromagnetic interference (EMI) can come in two forms: common mode or traverse mode. Common mode noise is created by a difference between power between ground and hot wires. Traverse mode noise has to do with a difference of power between the neutral and hot wires.

The other form of noise is radio frequency interference (RFI). This kind of noise is produced from equipment that utilizes electricity. Motors, elevators, electric magnets, electric space heaters, fluorescent ballasts, computers, and electrical cables (Stewart, J., Chapple, M., & Gibson, D. (2012).

There should be location considerations for these appliances. The more current that a piece of equipment uses, the more interference it can generate. Equipment that utilizes high amounts of current needs to be located away from all communications wiring to minimize interference.

4.2.2. Temperature, Humidity and Static Electric

Controlling the environment includes maintaining the facility climate. The heating, ventilation, and air-conditioning (HVAC) systems have to be monitored to that people are comfortable and the humidity is in a tolerable range. Computers need to have the humidity to be constant between 40 and 60 percent. Static electricity is produced when there is too little humidity and corrosion is caused if there is too much exists.

© 2016 The SANS Institute Author retains full rights.

4.3. Water

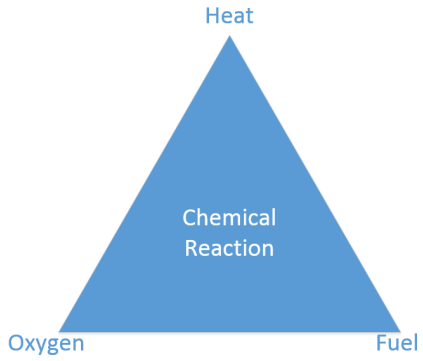
Water flooding and leakage can cause substantial damage to electronics and anything utilizing electricity, especially if in use. Electrocution may occur when people make contact water and electricity. Basements or near pipes carrying water should never house servers, data centers, and other critical electronics. The use of water sensors should be applied at important equipment locations so water is detected.

Safety and other personnel should be aware of water shutoff valves and drain locations to help lessen damage to facilities. The organization should be aware of how the site handles severe rain storms or flooding. Standing water should be removed as quickly as possible by having enough drainage.

4.4. Fire Prevention, Detection, and Suppression

Smoke, fire, heat, and detection systems need to be in place to protect employees from injury. Keeping people safe is most imperative objective of physical security. Suppression systems are put in place to limit the damage caused by smoke, fire, and heat. If too much suppression is applied, IT infrastructure and facilities can be damaged by these systems.

The fire triangle consists of three elements, Heat, oxygen, and fuel. The chemical reaction located in the center, represents what change occurs during fires. The figure below illustrates that if you remove any one of the four elements, Chemical reaction, oxygen, fuel and or heat, the fire may be eliminated.



Different methods are needed to combat the fire because of these elements. The temperature can be decreased by water and dry powders like soda acid, for instance, can subdue

© 2016 The SANS Institute Author retains full rights.

the fuel. Carbon monoxide is used to minimize oxygen and nonflammable gasses, such as halon or other equivalent substitutes, restrict with the chemical reaction and reduces the oxygen supply. Rapid fire detection and response is critical. Fires can quickly spread and the sooner the fire is detected, the easier it can be extinguished and reduce the damage caused by the suppressing agents.

Fire awareness training should be a mandatory part of physical security. Employees need to know evacuation routes to exit the facility and where to assemble so that attendance can be taken so that the safety employees know if any personnel is missing. Safety awareness training should include instruction on proper use and location of fire extinguishers. Training including CPR and first aid should be offered in case of injury.

4.4.1. Fire Extinguishers

Fires can come in different types. The sort of fire dictates what fire extinguisher is needed to suppress it. Using the incorrect fire extinguishers can intensify the fire. For example, in class B or liquid fires, water cannot be used because the liquid splashes and the chemical typically floats on water. Also, water can cause electrocution when there is an electrical fire. An important fact to remember is that fire extinguishers are only effective during the fire's infancy.

For class A, common combustibles fires, soda acid or water is used to eliminate fire. Class B, liquid fires, need carbon monoxide, halon or halon substitutes, and soda acid is used to contain these fires. Class C, electrical fires, must have carbon monoxide or halon or halon substitutes used for fire elimination. Class D, metal fires, should have dry power suppressants utilized for fire removal.

4.4.2. Fire Detection Systems

Fire detection systems need to be installed to protect the facility from fires. A fixed-temperature detection system alarms once a temperature is reached. Temperature sensors usually in a sprinkler head is melted the fire detector system is triggered. Rate-of-rise suppression systems are deployed when temperatures rise at a predetermined rate. Systems that utilize infrared technology to detect flames are called flame-actuated. Photoelectric or radioactive ionization sensors are utilized in smoke-actuated systems.

© 2016 The SANS Institute Author retains full rights.

Fire systems should be monitored by companies that call the local fire department in the event of an alarm. Sensors need to be properly located to detect fires. Detectors should be installed in private and public areas, the basement, raised floors, HVAC vents, server rooms, elevator shafts, and inside dropped ceilings (Stewart, J., Chapple, M., & Gibson, D. (2012).

4.4.3. Water Suppression Systems

Water suppression systems come in four types, wet and dry pipe, deluge, and preaction systems. Systems always full of water are called wet pipe systems. Pipes that contain compressed air initially are dry pipe. As air exits the system, water valves open, filling the pipes that dispense water. Another type of dry pipe systems is a deluge system. Deluge systems, have larger pipes that can douse fires quickly. Because of this, they are not recommended around server data center or other electronic equipment environments. A system that is a mixture of dry and wet pipe systems is called a "preaction" system. The preaction system rests as a dry pipe system to minimize the risk of water leaks. If fire or smoke is detected, the system fills the pipes with water and is dispensed if heat detection sensors melt inside the sprinkler head. Manual interference can stop the system from discharging water if the fire is extinguished. The preaction system must be reset and the pipes drained after discharged.

4.4.4. Gas Discharge Systems

People should never come into contact with gas discharge systems. Gasses that emanate from these systems displace oxygen and fill with hazardous gasses, making it inhospitable for humans. The type gasses that are used are carbon monoxide, halon, or halon substitutes. Halon is not manufactured because it depletes the ozone layer and is dangerous to people. If the fire it too intense, halon gas has a chemical reaction that creates a more toxic gas. If organizations have halon in their systems, they can still use it until the extinguisher is expired and cannot be refilled. Halon substitutes now include FM-200, NAF-S-III, argon, FE-13, aragonite, inergen and CEA-410.

4.4.5. Damage

Suppression methods like water hoses and soda acid for example, have to be taken into account when trying to extinguish fires. The materials used can cause corrosion or short circuit electronic equipment. Using the wrong method of suppression can cause the fire to intensify and spread instead of being contained. When firefighters respond to incidents, the axes used to get to

© 2016 The SANS Institute Author retains full rights.

fires and water hoses can cause destruction. Smoke and fire damage facilities and electronics. Hard drives if affected by smoke may be inoperable and high temperatures can destroy computer hardware.

5. Privacy and Legal Requirements

The organization should address employee safety in the security policy. Organizations must abide by laws and regulations that govern in the industry and jurisdiction they located. The company should practice due diligence to protect lives. If proper due diligence concerning physical security is not enforced by organizations, civil and criminal lawsuits could be filed.

5.1. Protection of Privacy

Personal identifiable information (PII) are specific details about people that include: name, social security number, phone number, address, age, religion, and race. Financial, medical and criminal records also are considered PII information. Organizations have a legal requirement to protect any PII information, and should not be collected without consent or for company profit. National Institute of Standards and Technology (NIST) outlines PII handling requirements within special publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* (McCallister, E., Grance, T., & Scarfone, K., 2010).

5.2. Legal Requirements

All organizations have imposed legal requirements. Jurisdictions and industry dictate the minimum foundations of what organizations are responsible. Human resources and legal departments are responsible for ensuring the organization is always abiding by laws and regulations. Safety guidelines, hiring limitations, classified information handling and software license use, include some of the aspects that these departments have to mandate to keep the company from being sued or fined from government agencies. Staying compliant is a key portion of sustaining a physical security plan.

6. Conclusion

Physical security requires planning to be able to protect the organization's assets. How the organization determines the priority of how resources are spent is through collecting data and

© 2016 The SANS Institute Author retains full rights.

identifying physical security key performance indicators. Metrics can be continually monitored and tracked after KPIs are identified to make sure that the company is making sound physical security choices that match the organization's threat model.

Administrative, technical and physical controls properly implemented allow the company to manage and protect resources. These controls should have the defense in depth approach that works together to provide multiple layers of defense, in case control is bypassed. Security measures help to deter, deny, detect, and then delay attackers from obtaining resources. Administrative controls include site location, facility design and construction, emergency response and employee controls. Physical controls include perimeter security, motion detectors, and intrusion alarms. Technical controls include smart cards used for access control, physical security intrusion detection systems, guards and CCTV systems.

Employees are the most import asset that physical security has the responsibility of safeguarding. To be able to accomplish this, basic facility needs such as, food, water, electricity and climate control must be available at all times. Employee safety should always be the priority and after that comes securing the facility.

In extreme cases like natural disasters, trained disaster recovery teams should to be prepared for these situations. In these circumstances, occupant emergency plans should be followed to help limit casualties. After human life is secure, business continuity planning and disaster recovery planning can recover the business and IT functionality.

Physical security is not always the first thought when it comes to security. Most organizations tend to focus on more technical aspects of security countermeasures. All the network intrusion detection systems and firewalls are completely useless if someone can get to the equipment and steal data or the device.

David Hutter, icewalkerdave@yahoo.com

© 2016 The SANS Institute Author retains full rights.

References

Scott, M. (2014, December 1). COCA-COLA DATA BREACH HIGHLIGHTS IMPORTANCE OF LAPTOP SECURITY. Retrieved December 3, 2015, from http://www.acfe.com/fraud-examiner.aspx?id=4294986501

Harris, S. (2013). Physical and Environmental Security. In *CISSP Exam Guide* (6th ed., pp. 427-502). USA McGraw-Hill;

Harris, S. (2013). Access Control. In *CISSP Exam Guide* (6th ed., pp. 97, 98, 157- 277). USA McGraw-Hill;

Harris, S. (2013). Information Security Governance and Risk Management. In *CISSP Exam Guide* (6th ed., pp. 21-141). USA McGraw-Hill;

Stewart, J., Chapple, M., & Gibson, D. (2012). Physical Security Requirements. In CISSP Certified Information Systems Security Professional study guide (6th ed., pp. 572-597,745-774). Indianapolis, IN USA: Wiley;

Oriyano, S. (2014). Physical Security. In Cehv8: Certified Ethical Hacker Version 8 Study Guide (pp. 393-409). Indianapolis, IN USA: Wiley;

Lynn III, W. J. (2010, September 30). Defending a New Domain. Retrieved May 17, 2016, from https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain

Santander Peláez,M. (2010 p. 6). Measuring effectiveness in Information Security Controls. Retrieved from SANS Institute website: https://www.sans.org/reading-room/whitepapers/basics/measuring-effectiveness-information-security-controls-33398

Boudriga, N. (2009). Smart Card Security: The SIM/USIM Case. In *Security of mobile communications* (pp. 141-142). Boca Raton, FL: CRC Press.

Olenewa, J. (2014). Radio Frequency Identification and Near-Field Communication. In *Guide to wireless communications* (3rd ed., pp. 392-395). Boston, MA: Cengage Learning.

Custom Electronic Design and Installation Association (CEDIA). (2008). Basic Electronics. In *Electronic Systems Technical Reference Manual* (1st ed., pp. 1-30). Indianapolis, IN: Author.

Wailgum, T. (2005, February 1). Metrics for Corporate and Physical Security Programs | CSO Online. Retrieved from http://www.csoonline.com/article/2118531/metrics-budgets/metrics-for-corporate-and-physical-security-programs.html

Irwin, S. (2014, September 8). Creating a Threat Profile for your Organization. Retrieved from https://www.sans.org/reading-room/whitepapers/threats/creating-threat-profile-organization-35492

David Hutter, icewalkerdave@yahoo.com

© 2016 The SANS Institute Author retains full rights.

McCallister, E., Grance, T., & Scarfone, K. (2010). *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* (SP 800-122). Retrieved from National Institute of Standards and Technology (NIST) website: http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

Anderson, M. A., Anderson, E. G., & Parker, G. (2013). Estimating and Scheduling Projects. In *Operations management for dummies* (pp. 261-267). Hoboken, NJ USA: John Wiley & Sons Inc.;

CNSS. (2010). *National Information Assurance (IA) Glossary* (CNSSI 4009). Retrieved from CNSS website: http://www.cdse.edu/documents/toolkits-issm/cnssi4009.pdf

Abbott, J. (2002). Smart Cards: How Secure Are They? Retrieved from SANS Institute website: https://www.sans.org/reading-room/whitepapers/authentication/smart-cards-secure-they-131

Hardy, G. (2012). *Beyond Continuous Monitoring: Threat Modeling for Real-time Response*. Retrieved from SANS Institute website: https://www.sans.org/reading-room/whitepapers/analyst/continuous-monitoring-threat-modeling-real-time-response-35185

U.S. Department of Homeland Security, & Interagency Security Committee (ISC). (2009). *Interagency Security Committee Use of Physical Security Performance Measures*. Retrieved from https://www.dhs.gov/xlibrary/assets/isc_physical_security_performance_measures.pdf

SANS Institute. (n.d.). SANS Institute - CIS Critical Security Controls. Retrieved from https://www.sans.org/critical-security-controls

Interagency Security Committee (ISC). (2015). *Best Practices for Planning and Managing: Physical Security Resources: An Interagency Security Committee Guide*. Retrieved from https://www.dhs.gov/sites/default/files/publications/isc-planning-managing-physical-security-resources-dec-2015-508.pdf

David Hutter, icewalkerdave@yahoo.com

© 2016 The SANS Institute Author retains full rights.