Utilizing Physical Security in Business Today
Vanessa Stanhouse
GSEC Version 1.4b Practical
Submitted September 8, 2003

Abstract

Over the last decade, technology has become an integral part of society, helping to increase productivity dramatically. Computers are utilized in grocery stores, banks, hospitals and schools. As the deployment of technology has progressed, society has become more focused on information security. While information security is critical to the survival of most companies and is necessary to protect consumers and businesses, physical security is still the foundation that needs to be maintained. Without physical security, the best forms of information security can be rendered useless. This paper will explore different forms of physical security and will clarify why physical security is crucial to maintaining information security.

Analysis

After the September 11th attacks on the World Trade Center, the business world began to shift its attention to the need for more physical security. Businesses began to focus on tightening security to prevent possible terrorists from harming employees, accessing their company data, or possibly destroying the buildings. Access restrictions were evaluated and updated, mail security was increased, and employee background searches became more thorough. Everything seemed to be headed in the right direction. However, as time progresses, the memory of what happened that day has become blurred by the need to move forward with life in general. As that memory fades, so may the focus on physical security.

In order to ensure that all information is properly protected, assurances must first be made that the equipment that holds the information is secure. When addressing the issue of physical security, the first step is to protect the building that houses the equipment. Buildings must be protected from natural disasters, including but not limited to earthquakes, lightening, tornados, hurricanes, earthquakes, and man-made disasters, such as train accidents, plane crashes, electrical transformer fires, automobile collisions, and fires. In order to ensure safety from disasters, the first consideration must be to ensure the structural integrity of buildings having business functions.

Structural Integrity

When reviewing structural integrity, the evaluation should begin with a review of the likelihood of each natural disaster. Buildings that reside in an area that has a high frequency of earthquakes should be built to withstand specific levels of movement just as buildings that are located within an area that is highly susceptible to tornados should be reinforced to withstand strong winds. Building codes will vary by region and generally take some of this into consideration, but extra measures may be taken at minimal cost to strengthen the structure.

When designing the building structure man-made disasters also require consideration. A weakness in building structure creates an avenue for an attacker to access the building while creating a distraction at the same time. These disasters can be as simple as breaking windows or as major as driving a car into the side of a building. All of this can be prevented by simple upgrades to the building materials, some design modifications to the building and the area around the building, and a few minor additions to the structure. Basic upgrades should include reinforced walls and anti-theft glass.

There are many new building materials that incorporate security features into their design. One example of this would be the recent development of anti-theft glass that incorporates a sensor into the glass. When the glass is broken or cracked, an alert is automatically sent to a monitoring service. The glass is also protected with a special layer of film used to hold together two separate layers of glass, making the glass more difficult to break. Window tinting, to prohibit possible attackers from viewing secure information and internal physical security features from outside of the building, and soundproofing should also be considerations when selecting the proper glass for the building.[1]

To deter direct physical attacks using a motor vehicle, exterior design features should also be considered. Attackers will use any method necessary to gain access to the information that they want to either posses or destroy. This could include driving a car through the side of a building or planting an explosion in a near-by field or parking lot. While this may seem a little drastic, there are cases where this has happened, as witnessed in Oklahoma City in 1995[2]. Obviously, the situation will all depend upon how vital the information is and the determination of the attacker. Another aspect to keep in mind is that an attacker may not actually be the person that performs the act. Meaning, the attacker may solicit a disgruntled employee or an estranged spouse to actually cause the damage to the building, thus creating a window of opportunity for the attacker. Utilizing simple design features such as concrete decorative planters, statues with bases that are recessed underground, or trees will help to increase protection of the building. Curving roadways and adding speed bumps will also help to deter drivers from obtaining damaging speeds.[3]

[1] Asia Times http://www.atimes.com/atimes/Japan/EF07Dh02.html
[2] CNN Interactive http://www.cnn.com/US/OKC/bombing.html
[3] U.S. Security Associates, Inc. http://www.ussecassoc.com/public/docs/buildingsecurity.htm

Access Controls

Controlling the access to the interior of the building is a key element to the physical security of the equipment located within a complex. In order to properly protect equipment and data, numerous layers of security should be utilized to control and monitor access to the areas in question. Some forms of access controls include badge/key readers, hard keys, combination locks, cyber locks, biometric readers, stationed security guards, solid, non-moveable walls, and non-accessible floors and ceilings. Unauthorized access through windows should also be evaluated.[4]

The most common form of access control is the standard hard key lock. With the hard key, similar to what is used with most homes and automobiles, access is restricted to only those that actually posses the key or those that can pick or break the lock. Hard key locks vary by size, material, and design. The locks range from a basic security lock, as seen in the average home, to a high security lock. High security locks often feature the ability to reprogram the lock if a key is lost. They are also usually made of durable steel making it more difficult for an attacker to "drill" the lock. Another feature of the high security locks is the set of pins called sidebar pins that interrelate with special side cuts on the keys. When the keys are inserted into the lock, the sidebar pins are all raised to fit the distinctive side cuts on the key, allowing the key to continue entering the lock. If all of the "regular" cuts on the key are correct as well, then the key will be able to open the lock. If either of the cuts is incorrect, sidebar or regular, then the cylinder will not turn. This type of lock is considered virtually pickproof. Unfortunately, the hard key is still exposed to common human error. If the key is lost or stolen, then the company faces a potential security breach that must be addressed.

The cost of a hard key lock can range from low to moderate depending upon the design/style of the lock. Most small companies will consider the hard key lock to be the best option due to the low cost. There is a cost for the purchase of equipment and installation, and an additional nominal cost for duplication of keys for each end user and also to replace lost or missing keys. Moreover, the company may have to pay a re-key cost similar to the installation cost if the security of the lock has been compromised or is in danger of being compromised.

Another type of lock is the combination lock. Combination locks can be used alone or in conjunction with a hard key lock and are normally re-programmable in the event that a security breach has occurred or is suspected. This may cause inconveniences when trying to inform the employees of the new combination, but the inconvenience is normally worth the ability to ensure continued security. Another disadvantage of combination locks is the users'

[4] CardWerk http://www.cardwerk.com/smart-card-solutions/physical-access-control/

capability to remember the combination. If the users are required to remember numerous passwords, they may not be willing to attempt to remember another set of characters for access into the room. Most combination locks also do not have the capability to record entry times, dates, or employee names.

To have the capability of recording access information, the option of either cyber keys or a badge/key reader should be considered. While both utilize electronic programming to control and record access, there are differences. The cyber key utilizes a standard door lock configuration with an electronic cylinder in the place of a standard hard key cylinder. The key provides the power source for the cylinder and can be programmed to only allow access at specific dates and times. Both the key and the lock record access attempts and can be downloaded for viewing.[5]

The badge/key reader normally requires installation of a special device that reads the identifying information from the badge/key, such as a bar code or magnetic strip. The initial cost of the badge/key reader system is significantly higher than the standard hard key lock. Depending upon the sophistication of the badge reader system, the price range may vary from moderate to high; however, the cost to re-key is eliminated, due to the programming possibilities of the readers. In addition to the standard badge/key reader, there is the option of a proximity badge system.

The proximity badge reader allows the user to hold the badge in proximity of the reader rather than having to swipe the card through a device, eliminating the normal wear on the device and the need to maintain the reader heads in the device. The reader constantly transmits a low level fixed RF (radio frequency) signal that transmits energy to the badge. When the badge is held near the reader, the RF signal powers a chip located within the badge. This chip contains a unique identification code, which is then transmitted back to the reader. The reader can be concealed inside walls or special enclosures or surface mounted directly on a wall. The badges are virtually impossible to duplicate and can usually be read through a purse, briefcase, or most nonmetallic materials.

If preferred, a company may choose to utilize a stationed security guard at the door. This may be in addition to previous mentioned forms of access control or as the single access control point. Security guards provide a back-up option in the event of malfunction of the reader device or in the event of an emergency. Also, having a security guard provides an additional layer of security if the badge/card includes photographic software. With the photographic software, as the person utilizes the badge, a photo of the badge owner appears on a computer monitor located with the security guard. The guard is then able to confirm if the person that used the badge is the actual owner of the badge.

[5] Star Safe & Lock http://www.starsafe.net/prd_accesscontrol05.htm

Regardless of the type of lock chosen, the style of door must also be considered. A secure door must have a self-closing mechanism to prevent the possibility of a door being left ajar. This will prevent the possibility of both accidentally and intentionally bypassing the security, such as badge readers, that have been put in place. If the door is located in a high traffic area, a turnstiles door may be necessary to prevent tailgating or piggybacking.

To take the security of an area a step further and to address security from the reactive side, the implementation of a video camera system should be evaluated. In the event of a security breach, the camera would provide a photographic log of the person that breached the system. This would help to identify the person and the means that they used to penetrate the system. A security camera also offers an additional level of security by providing the option to have a physical person monitor the door from a remote location.

Biometrics

Another form of access control is biometrics. Unlike the previously mentioned forms of access control, biometrics can be used for authorization, authentication, and identification. As the level of security breaches increases and attackers become increasingly more creative, the need for highly secure identification and personal verification technologies is becoming more apparent. Biometrics can measure a wide variety of individual traits such as: facial features, fingerprints, hand geometry, handwriting, iris, retinal, vein, and voice. Forms of biometrics include:

- *Facial Recognition* – Utilizes a multi-scale algorithm to detect and record faces in a crowd. The faces are then compared to a database for identification.
- *Facial Thermoscan* – Similar to facial recognition with the addition of the measuring of the temperatures of the face.
- *Fingerprint Scanner* – Identifies key points of a fingerprint and references those points with a database for identification.
- *Hand Geometry* – Identifies specific hand measurements for shape and size.
- *Signature (Handwriting) Verification* – Compares handwriting styles, pen speeds, and pen pressures to samples
- *Iris Scanner* – Compares the unique features of the texture and patterns of the iris
- *Retinal Scanner* – Identifies the unique pattern of the blood vessels at the center of the retina

- *Voice Recognition* – Evaluates voice patterns, including tone, pitch, rhythm, and accents

With biometrics, the opportunity for an attacker to steal a badge or keys is virtually eliminated. Biometrics is based upon personal traits that are digitally recorded and stored and cannot be easily replicated or modified. These biometric identifiers can be stored or converted to digital form and embedded into "smart" credentials and ID cards. Smart cards integrate a circuit chip that performs sophisticated cryptographic functions and stores biometric patterns tied to the user's unique biometric data.[6]

Fingerprint Scanning

Fingerprint scanning is one of the oldest forms of biometrics. Using a charge coupled device (CCD) similar to that of a digital camera, the fingerprint scanner shines a light on the finger, illuminating the ridges of the fingerprint. The system then creates a reverse image of the print showing the darker areas representing more reflected light (the ridges of the finger) and the lighter areas representing less reflected light (the valleys between the ridges). Key features of the fingerprint, such as points where ridge lines end or where one ridge splits into two, are identified and marked. The device then digitizes the fingerprint layout on a template that is stored in the system for later use. The next time that person needs to be identified; the new scan is verified against the template already created. This process can be enhanced by the addition of three dimensional analyses for verification, thermoscanning to verify an acceptable temperature, or infrared detection that ensures that there is a pulse present within the finger itself. This greatly reduces the chances of a security breach using a fake finger made of gelatin or other materials.[7]

The fingerprint scanner is used today in some ATM machines and is gradually increasing in usage in various other circumstances. Fingerprint scanners are being used in airports to increase security and police stations to in replacement for the old ink and paper identification process. These scanners are also now available for use with personal computers at a cost of less than one hundred dollars for a USB device. When used in addition to a secure password or another biometrics device, this can greatly enhance the protection on any computer system.

Properly implemented, fingerprint scanners offer a potential for high accuracy, the readers tend to be diminutive (easily incorporated into a keyboard or a mouse), and they have a relatively low cost. However, some potential problems can arise because cuts, dirt, or scars on the finger can cause some systems not to recognize a valid fingerprint. Some scanners also require precise placement of the finger, invalidating a finger that is not properly aligned with the scanner.

[6] Java World http://www.javaworld.com/javaworld/jw-12-1997/jw-12-javadev.html

[7] How Stuff Works http://computer.howstuffworks.com/fingerprint-scanner1.htm

Facial Recognition and Facial Thermoscan

Facial recognition and facial thermoscan are both fairly new in the biometrics realm. With facial recognition, the system uses a camera to capture the image of a person's face and compares that image to one that is stored in a database. The device then measures up to 40 facial characteristics such as the distance between the eyes and is not affected by facial expressions. Thermal imaging techniques analyze the heat-generated pattern of blood vessels underneath the skin. Both technologies are attracting a great deal of media attention with the recent implementation of these systems for airport and border security in identifying wanted criminals and terrorists.[8] Facial recognition systems have also been used in recent years at the Super Bowl to scan for known criminals.[9] The attraction of these biometric systems is the ability to operate "hands-free", limiting the amount of man-machine interaction.

While it is not complicated to compare and match two static images, picking an individual out of a group, as some systems claim to have that capability, is another matter. For example, if the systems are 99.99% accurate, and one out of every million flyers is a terrorist that leaves 999 people potentially wrongly identified at security checks. Other flaws include the systems' inability to account for the affects of aging, to recognize a person who changes from wearing to wearing contacts, to recognize the subject after a haircut, and to distinguish twins or triplets. Since the technology is still in its infancy, there will continue to be improvements and there should be great strides being made every year to improve accuracy.

Hand Geometry

Hand geometry, which is one of the most established methods of biometrics, measures the physical characteristics of the user's hand and fingers. The theory of hand geometry is based upon the fact that virtually every person's hand is has a unique shape which does not significantly change with age. When the user places a hand on the scanner, an image of the hand is captured, and the shape and length of the fingers and knuckles are measured. This process typically offers a good balance of performance, usability, and accuracy. Hand geometry is most widely used in physical access control and time/attendance systems. One drawback to the hand geometry system is the requirement of a large size scanner, which has hindered its deployment with many computer security applications.

Signature Verification

Another form of biometric identification is the use of signature (handwriting) verification. The use of a signature has been widely accepted throughout time on correspondence, legal documents, and financial documents and has built a foundation of confidence in a signature based verification systems. With automated signature verification, the user signs his signature on a

[8] American Civil Liberties Union http://archive.aclu.org/issues/privacy/facial_recognition_faq.html
[9] RAND http://www.rand.org/natsec_area/products/ip_biometrics.html

digitized graphics tablet. Signature dynamics, such as speed, stroke order, stroke count, letter shape, height and distance, timing, and pen pressure are analyzed. Computer software can then differentiate between the parts of the signature that are habitual and those that vary each time.

Problems exist however with signature recognition. Repeatability of the signature and the recording ability of the devices used in the recognition process have limitations. The Dynamic Signature Verification (DSV) system can adapt to variances in the signature dynamics. Even with these verification systems, variability with signatures make it difficult to consistently use signatures for verification and authentication.[10]

Iris Scanning

Iris recognition systems use a video camera to capture a sample of the iris while special software compares the resulting data against previously stored templates. With iris scanning, direct contact with the scanner is not necessary since the iris (the colored part of the eye) is visible from a distance. The user is also not required to remove eyeglasses, and the scan is not affected by contact lenses, either traditional or colored. The technology works by scanning the unique random patterns of the iris starting by finding the right and left outer edges and then the inner edges at the pupil. The system does not utilize the top and bottom of the iris since these areas are normally hidden by the eyelids. Even though only a small portion of the eye is able to be scanned, every iris is unique. The system then converts the characteristics of the iris into a code that is stored in a similar manner to the fingerprint scan.

Retinal Scanning

Often confused with iris scanning is retinal scanning. With retinal recognition, a low-intensity infrared light is directed into the front of the eye to illuminate the retina, which is layered with blood vessels located at the back of the eye near the optic nerve. The unique features of the vessel pattern are measured and recorded. Retina biometrics is considered to be the best biometric process. However, despite its accuracy, this technique is often thought to be inconvenient and intrusive making it difficult to gain general acceptance by the user. Another drawback is that the user must look directly into the retinal reader in close proximity. This is inconvenient for eyeglass wearers. There may also be concerns with the spread of infections because of the physical contact required with the retinal scanner. Retinal scanners are also ineffective with the blind and those who have cataracts.

Voice Recognition

[10] findbiometrics.com http://www.findbiometrics.com/Pages/signature%20articles/signature_1.html

While voice recognition is the most convenient biometrics application, it is also the least reliable due to the risks of impersonation, remote access and poor accuracy levels. Background noise, microphone quality, or vocal changes due to anxiety, a cold, laryngitis, or dental problems may also cause recognition problems and false rejections. Voice recognition measures the unique variations in a person's speech pattern and verifies that person's identity on the basis of their voice characteristics. The unique features of the user's voice are then digitized and compared with the individual's pre-recorded "voiceprint" sample which has been stored in a database. One of the largest applications for voice recognition is for telephone-based verification scenarios.

Environmental/Life Safety

In addition to access controls, you must have certain protection controls in place to protect your assets and to prevent a security breach. Computer systems and employees require a controlled environment. Controls for this environment may include fire suppression systems, ventilation, air conditioning, and heat. While it is rational to expect that protection against disasters, fire, flooding, explosions, and natural disasters, will be provided to the best of the company's abilities; additional measures are necessary to protect the company's data and equipment. The risks to the data in the event of a disaster will depend upon the vulnerability of the storage devices after a facility is damaged due to a natural disaster, causing malfunctioning or irrelevant security devices (i.e. badge readers on a door with a large hole in the wall right next to the door). Some risks that may arise from a disaster would include damage caused by weather, firefighting techniques, vandalism, theft, heat, and salvage operations. To decrease the threat of a security breach, a company should ensure that they have proper contingency plans in place for each scenario.

Physical Security and Information Security

Regardless of the levels of information security, if a computer system is not physically secured, the information security is rendered useless.[11] Once the physical security of a system has been compromised, the equipment is subject to the capabilities of the attacker. If the user has not protected the system with a password or has forgotten to lock the system, the attacker has instant access to all unencrypted information on the computer. In order to bypass password protection, the attacker simply needs to insert a boot disk into the computer and power the system on. Once the system powers on with the new operating system, the password is bypassed and the attacker has access to the information just as if there was no password. The attacker can also achieve access to the system through the utilization of password cracking software (i.e. LC4[12]). Both of these situations give the intruder the ability to release viruses or attacks against

[11] http://www.cccure.org/Documents/HISM/675-680.html
[12] @stake http://www.atstake.com/research/lc/index.html

the network from the inside; bypassing any security measures such as firewalls that may be in place.

Without physical security, intruders also have the capability to install devices such as key loggers (i.e. KeyGhost[13]), video cameras, and tape recorders. Once these devices are installed, the attacker can utilize any information acquired. This information may include passwords, company confidential and proprietary information, and confidential customer data. In order for a company to operate with a level of trust and reputation, it must maintain integrity, confidentiality, and availability. Without these three objectives, a company can not be successful.

The level of security needed will vary depending upon the data and equipment that must be secured. Each different situation must be individually evaluated, with the allowance for exceptions and specialization. An example of this would be the security of an investigation team. In order for the team to meet the requirements from a legal, an ethical and a privacy standpoint, the team would need to be within a secure area to maintain confidentiality and preservation of evidence. If this is not possible, the team may not be able to effectively complete an investigation.

Conclusion

As technology has become entwined with our everyday lives, the need to secure the private and confidential information that is stored on computer systems has become a necessity. In order to sufficiently protect the information and the computer systems that hold it, businesses must first consider the many options that are available with physical security, including structural integrity, access controls, and environmental/life safety systems. Without physical security, the guarantee of information security can not be achieved.

[13] KeyGhost http://www.keyghost.com/sx/

References

1. "Secom, Asahi developing anti-theft glass." Asia Times Online. June 7, 2003. http://www.atimes.com/atimes/Japan/EF07Dh02.html accessed on September 8, 2003.
2. Cable News Network, Inc. "Oklahoma City Tragedy: The Bombing." 1996. http://www.cnn.com/US/OKC/bombing.html accessed on September 8, 2003.
3. Pitts, T. "Building Security – Checklist." 2002. http://www.ussecassoc.com/public/docs/buildingsecurity.htm accessed on September 8, 2003.
4. Jacquinot Consulting, Inc. "Physical Access Control: Secure Access to Buildings and Spaces." September 1, 2003. http://www.cardwerk.com/smart-card-solutions/physical-access-control/ accessed on September 8, 2003.
5. "Cyber Lock Systems: Innovative access control system." 2002. http://www.starsafe.net/prd_accesscontrol05.htm accessed on September 8, 2003.
6. Di Giorgio, R. "Smart Cards: A primer." December 1997. http://www.javaworld.com/javaworld/jw-12-1997/jw-12-javadev.html accessed on September 8, 2003.
7. Harris, T. "How Fingerprint Scanners Work." http://computer.howstuffworks.com/fingerprint-scanner1.htm accessed on September 8, 2003.
8. American Civil Liberties Union. "Q & A on Facial Recognition." 2002. http://archive.aclu.org/issues/privacy/facial_recognition_faq.html accessed on September 8, 2003.
9. RAND. "Super Bowl Surveillance: Big Brother or Beneficial Technology?." http://www.rand.org/natsec_area/products/ip_biometrics.html accessed on September 8, 2003.
10. "Understanding Signature Verification." http://www.findbiometrics.com/Pages/signature%20articles/signature_1.html accessed on September 8, 2003.
11. "Domain 10: Physical Security." CISSP Open Study Guide Web Site. http://www.cccure.org/Documents/HISM/675-680.html accessed on September 8, 2003.
12. "LC$ - The Password Auditing and Recovery Application." 2003. http://www.atstake.com/research/lc/index.html accessed on September 8, 2003.
13. "KeyGhost: Powerful Internal Security and Audit Tool." http://www.keyghost.com/sx/ accessed on September 8, 2003.