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

Best Practices for Securing Office Facilities: An Introduction to Physical Security

Tim King
GIAC Security Essentials Certification
Version 1.4b, Option 1
February 2004

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Abstract

The purpose of this paper is to give the reader a good foundational understanding of best practices for physically securing remote offices and/or corporate branch buildings/facilities.

A recent study by marketresearch.com, a leading multinational research organization, pointed out that building architecture in the private sector faces potential threats from violence/terrorism, corporate espionage as well as the obvious concern, theft (Frost and Sullivan). As such, the need for Electronic Access Control (EAS) has become increasingly important in construction and updating of today's facilities, particularly those housing sensitive data, as well as computers and data transmission equipment. But EAS is just the focal point of a significant number of techniques for physically securing facilities from malicious attacks and thefts, both data and physical.

The American Institute of Architects places an excellent checklist in its brochure, "building security through design" (see Works Cited), and provides information that building planners should use in determining the security risks related to that facility.

The following are several areas in which building and facility planners, as well as corporate and computer security personnel should take into consideration when preparing and building new structures or updating old ones.

1. Bells and Whistles

Arguably the most important aspect of building security is an effective and appropriate alarm system. But facility security is incomplete without a system that is specifically designed to alert local authorities. Though it is beyond the scope of this dissertation, a multi-use police *and* fire system can provide additional benefits in terms of safety and facility asset protection. Though there are numerous types of alarm systems, recommended is one that features the typical door and window sensors, as well as motion detection equipment. Recently, motion detection equipment has become pivotal to providing awareness of intruders who may have slipped past more conventional security measures, especially when facilities are unoccupied.

Depending on the type, motion detection equipment can alert authorities and/or activate security recording equipment, which is useful both in prosecution and identification of suspects, as well as providing information on what malicious activities a perpetrator may have engaged in.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

And there are other forms of alarm sensors, including pressure sensors in flooring, seismometers, microwave and laser beams, passive infrared, and simple electrical sensors on windows and doors (Thames).

2. Entry from Above

Though it is often thought of as the material of high-tech spy movies, the drop ceiling represents a significant risk in terms of access to sensitive/restricted areas. As such, barriers to the use of such spaces should be an issue that no planner should overlook. Drop ceilings are potential entry points when other conventional routes are highly secure. Many security organizations and consulting firms suggest that among other obvious recommendations—solid walls, lock systems, etc.—we must also avoid drop ceilings that permit individuals from moving from room to room, when such access is normally prohibited by other forms of access.

Options for the perimeter walls around highly secured rooms;

- Deck-To-Deck metal stud wall
- A perimeter security barrier to prevent unauthorized access through drop ceiling

The Texas Medical Association in its review of building security measures recommends looking at several other similar access points like ventilation systems, windows and fire escapes (Texas Medical).

3. Better Bolts

We can easily overlook the main way in which security might be compromised—The Front Door—but we should be mindful that even the best conventional locks may be subject to picking through the use of any of various tools available to the criminal. Some of these range from the small multi-size picks, popularized in television crime dramas, to more sophisticated devices that adjust themselves to match tumbler sequences within a lock's core. Because of this potential, tamper-resistant locking systems, including tamper-proof strikerplates, are paramount to the first line of defense. As has been utilized in many larger apartment buildings, an added method includes an "airlock" style entryway in which entrants pass through a pair of security doors, a method that is employed widely in European banking institutions.

When using conventional key-access locks, some, such as the security wing of the Thames Valley Police, recommend the use of "suites" of keys. These are keys that open several different doors throughout a facility, but can be engineered to offer more minimal/limited access to those with lesser security ratings (Thames). It is important to suggest that in the modern age, digital code locks are more desirable than traditional tumbler locks. These unlocking systems have the advantage of being able to chance access by changing codes at any

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

time. Codes should, however, be changed regularly to minimize risks caused by the viewing of passers-by and other unauthorized personnel (Ross).

A final means of entry that is appropriate to our discussion is that of card entry. Because of its flexibility and ease of replacement, this may be among the best forms of entry-access. The greatest concern in swipe card technology, which may incorporate magnetic strips or even barcodes, is that lost cards become potential security threats. With the most up-to-date technology, however, this concern is largely unfounded. Upon the report of a lost card, the coding for that employee's card can be removed from the system as invalid and new media issued. Additionally, the swipe card is often combined with conventional redundant means, such as the holder's photograph and other identifying information. The Thames Valley Police, in their expansion on the topic, points out that with today's systems, cards can be expanded to allow exit-only use for use by cleaning personnel, as well as more limited location access privileges for guests, visitors and vendors.

4. Picture Perfect

In the modern day, virtually no one protecting a sensitive facility would imagine not utilizing some sort of visual monitoring system. But just as important as monitoring the internal workings of the facility itself is the placement of cameras on entryways into the building. Additionally, these cameras should be of the recording type, even if there is human monitored camera operations elsewhere in the facility. Having a record on tape or digital ensures identification of both criminal and authorized individuals.

Closed Circuit Television, or CCTV, is not the end-all answer to good security, but provides an excellent tool when combined with other building security methods discussed in this composition (Ross).

Organizations must analyze their goals prior to jumping into a monitoring system. As mentioned above, will the building simply require a cycled recording of the goings-on? Will it need 24-hour observation? Will it need just an image of an entryway, or shots throughout the facility? All these factors relate to costs, as well. Some experts now suggest the use of a remote monitoring facility, such as is offered by external security firms, as a means of keeping expenses down. The use of monochromatic versus color, the ability to tilt-and-pan, and evidentiary resolution also become important factors in selecting the type of system (Thames).

5. Signs Everywhere

It goes without saying that only authorized people should be in restricted areas and/or facilities, however it is critical that those areas be flagged off with

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

appropriate signage indicating such. Doors should typically state “Authorized Personnel Only.” The benefits of such admonitions are twofold:

1) It is an aid in prosecution, should unauthorized entry come to that point; and

2) It provides a necessary reminder to unauthorized employees that such areas are off-limits without appropriate security clearance (AIA).

Gensler Architecture recommended placing records—a high security issue, further away from public access points, while public areas were closer to egress points. Here a security issue was covered at the same time as a public safety concern (Kirkpatrick).

6. Who’s Who

Securing a facility transcends the physical security structuring of the building—It also encompasses how we authorize access to those within the organization. Areas need to be divided into levels of access. This concept can be viewed in analogy as concentric circles. The outermost layer requires the least stringent security, i.e., all employees may enter. The next circle requires more sophisticated means of entry, swipe cards or pass codes, for example. As we go in closer to the central bulls-eye of our circle analogy, more protection is employed, such as biometrics for entry, additional locking systems, and more thorough monitoring equipment. Developing multiple levels of security for employees simplifies this task. An example of restricting various areas inside of a facility is as follows:

Installing a dual key entry system, where;

- First key will get access to main building
- Second key will grant access to a server/network room

The following rings/zones of security can be put in use:

- Ring/Zone 1 limited building access to authorized employees or associates (First Key)
- Ring/Zone 2 electronic key-access to the server area/network area/etc... Access should be limited to those with a valid work requirement only (Second Key)

Finally, in conjunction with this concept, one physical item may become important, and that is the lack of window view from the outside for the most secure areas (AIA). Just as a casino will never have a public window to the counting room, neither should computer or banking operations.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

7. Tying up Loose Ends

As we discussed, in terms of having fire protection in conjunction with police notification, so should we protect our vital data by ensuring that all networking cabling be protected from breakage or disconnection. Many newer facilities are very network friendly and are designed that way. However, older structures may necessitate the passage of various cabling across flooring or along walls.

Those on floors, especially, represent both a risk to network connectivity but also one of safety. Cable floor strips prevent tripping, as well as the accidental dislodging of wires. Bright yellow safety tape aids in reminding employees to be cautious when walking around these areas.

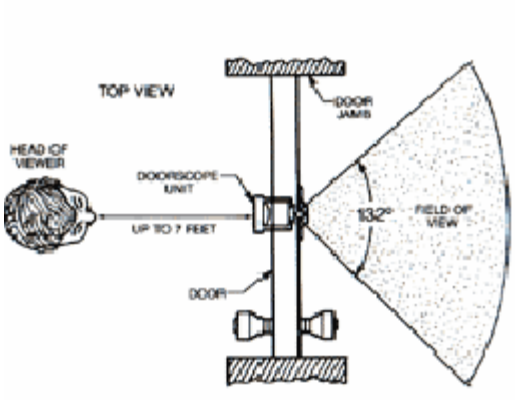
Finally, organizations need to review both the sensitivity of the type of data they are transmitting across lines, as well as the type of cabling they are using. Should it merit high security, these lines may need to be run through walls or through conduit (either in the walls or in the flooring) to avoid potential lapses in security due to passive monitoring or splitting of cables by hackers who would eavesdrop on communications. Of course, appropriate encryption technology, though beyond the scope of this study, would alleviate some of the risks involved therein.

8. Take a Look

Those high security areas and/or buildings are recommended to have one-way peepholes, or spy-hole viewers, on doors to allow interior occupants to verify the authenticity of those attempting entry, while not compromising internal operations to curious parties. This simple, passive method is one of the surest methods and can provide an excellent line of defense in the event that other technological means break down.

Some newer peepholes even allow those on the inside to view the other side of a door from up to six to seven feet away and give a very wide fisheye view to make visible intruders who attempt to hide on the side, “leaving no dead zones,” according to the marketers of one such device, the DoorScope. Others like the UltraVision and WideVision can provide angles as wide as 132° (still others exceed a 160° view) and liken themselves to “a miniature color video monitor installed on the door” (Advanced Safety).

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



(Advanced Safety)

These devices can cost as little as $16-$30 and can be installed by the facility's own maintenance staff. Additionally, they can be retrofit on existing doors (Peep Hole Security).

9. Out in the Open

To limit possible intrusions by malicious hackers or potential inadvertent damage by the general public, non-secured areas should be free of any network connections. Though this concept is probably common sense, it nonetheless merits reconsideration when designing secure facilities that also have public areas. Also, be certain that any landline telephones in public areas are not carrying any kind of network or ADSL-type inaudible signal. Even hardwired telephones might be compromised by the use of conventional modems attached to the phone transceiver, though this is unlikely.

10. Testing

Finally, scheduled and unscheduled testing of a facilities physical security measures should be completed. Testing can be completed by trained internal employees or more often, consultants are hired to perform these physical penetration tests. Some benefits of having an outside group perform physical penetration tests are:

- No prior knowledge of existing physical security implementations
- Tester is not known to internal personnel
- Reporting can be published directly to management for Risk Analysis

Performing regular physical security penetration tests illustrates how easily physical perimeter security can be bypassed. By simulating real world intrusions,

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

an organization can gain an effective way to test for security vulnerabilities, as well as determine how well monitoring and response capabilities are operating.

Features and benefits of physical security penetration testing include:

- Provides a snapshot of security vulnerabilities in the physical perimeter which means that an organizations decision makers can quantify the risks to which the facility is exposed

- The penetration test results can provide recommendations on how to correct each vulnerability

- Typically, vulnerabilities are reported in non-technical verbiage, allowing non-security experts to understand the content and concepts

- Provides recommendations, which means that management can improve their detection and response strategies

Completion of regular physical security penetration testing allows for measurement of the effectiveness of your overall physical security approach, monitoring and also evaluates an organizations ability to respond to various incidents.

Conclusion

In this paper, we have explored some of the basic practices for physically securing facilities. We examined how an active monitoring system in conjunction with motion sensing equipment is one of the most effective security measures that can be taken. Also, we explored how drop ceilings can be a point of unauthorized entry and that security locks in addition to video surveillance (CCTV) helps to complement the overall security of a facility. Next, we looked into how appropriate signage and dividing facilities into 'Zones' can reduce employee confusion while raising awareness of restricted areas within the facilities. Additionally, we examined how regular physical security penetration testing can aid an organization in its efforts to expose security deficiencies.

Inasmuch as we would like to make the assumption that all buildings will be secure based on personal honesty and the deterrent of prohibiting entry based on the simple request to the unauthorized, we must be realistic and employ all reasonable means that will protect our material and digital assets.

The solution to effective facility security follows the working airplane analogy. Just as most crashes occur due not to one failure, but a cascading chain of events, so must we secure our buildings with redundancies and multiple means.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Of course, none of these business and facility security methods supercedes the critical process of training and instructing employees in effective practices. The University of Wisconsin's Building and Office Security procedures expand on the physical plant to have workers be aware of unfamiliar persons, to protect access codes and change them regularly, to know what is out of place (University of Wisconsin).

Gensler suggests that we must use evenhandedness when preparing the security aspects of facilities. It is human psychology to become more resistant and more lax when systems become too complicated. This is where automated processes and procedure, as described in this paper, help to bridge the gap.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Works Cited

Advanced Safety Devices. “Doorscope.” http://www.safety-devices.com/doorscope.htm

American Institute of Architects. "building security through design." 2001.

Anderson, Ross J. *Security Engineering*. John Wiley & Sons. 2001.

Frost and Sullivan. *U.S. Electronic Access Control (EAC) Systems Markets*. Study Published by Marketresearch.com. 1 September 2001.

Kirkpatrick, Kate. "Integrating security into office buildings." Gensler Architecture. 2001.

Peep Hole Security. “Who is Outside Your Door?” http://www.minitronics.com/phs/

Thames Valley Police, U.K. “Business Crime.” http://www.thamesvalley.police.uk/business-crime/index.htm

Texas Medical Society. “HIPAA Security: You Can Run, But You Can't Hide.” http://www.texmed.org/cme/pms/ec_pmsem/hipaa/physical_safeguards.asp

University of Wisconsin. "Building/Office Security.” http://www.uwpd.wisc.edu/Awareness/Building.htm

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.