Global Information Assurance Certification Paper

Abstract

This guide presents a comprehensive approach to securing your information in the real world. Information is provided on securing the overall facility, server rooms, equipment, and digital media.

A layered, or defense in depth, strategy provides the best possible security for your information in the electronic environment. The same approach to your physical security will provide the best possible protection for your information systems in the physical environment.

Introduction

The security of your information is only as strong as the weakest link in the chain. A firewall is bypassed with a modem. E-mail virus scanning is side-stepped with file sharing programs. And the most stringent NTFS file access control list is brushed aside with a bootable floppy.

Although security in the virtual world is critical, ignoring or downplaying physical security is just asking for trouble. The primary physical security threat is people inside your organization. This does not mean, however, that you can completely ignore the external threats to your systems either.

Unfortunately, the predominate physical threats to your information systems - uninformed users and disgruntled system administrators - will easily pass through your external physical defenses. Depending on the value of the information you hold, however, there may be plenty of people who would risk a break in to gain access. Financial institutions come to mind first. Telephone companies, Internet data centers, government and military agencies also top the list of places that are under a real external physical threat.

Even if you don't process military secrets or handle vast sums of money on a daily basis, you might still be surprised by who would want to do your company harm. Probably the primary objective in this case would not be to steal information, but to deny you access to it. Imagine an insurance agency customer who was turned down on a claim and decided to get even by damaging systems while everyone is at lunch. Or a lawyer's client who decides his legal interests would be best served if his records just disappeared.

Facility Security

The building that houses your information technology provides your first line of defense against physical attack. Much as a firewall is the first checkpoint a network intruder will encounter when trying to gain access to your systems, the external perimeter of your facilities is the first barrier to physical intrusion.

Let's turn our attention to the physical structure that houses your information systems. We'll first examine the building itself – the walls, doors, and roof - and then turn our attention to auxiliary systems such as fencing, access control systems, surveillance systems, and alarms.

Most companies already have a physical presence and varying degrees of thought went in to the physical security aspects of their location. Whether you're planning on moving in the near future or you're fairly certain you'll remain where you are will influence your physical security decisions. Some security precautions are easy to implement during initial construction, but may be hard to retrofit afterwards.

Doors
The door is the most common point of entry into your facility. How well are your entrances able to stand up to a forced entry? While a glass door may present an aesthetically pleasing appearance, it may not be the best choice for a main perimeter door. One option that combines aesthetics and functionality is to use a glass door for the entrance into a reception area and then use a heavier solid core door to protect the entrance into the main office space.

While a solid wood door will suffice for most applications, a heavier door may be appropriate in other circumstances. A solid wood or composite material door with an outer covering of steel will provide much better resistance to intrusion than the typical interior doors found in offices today. By moving the “exterior” perimeter just inside the reception area a much stronger defense can be constructed while maintaining a pleasing appearance.

One other consideration when using this approach is to consider what information is available in the reception area. If the receptionist has a personal computer with lots of valuable information on it, then it becomes a high value target itself. You can reduce the value of this machine by placing it outside any network defenses and requiring it to use a secured VPN connection to access any information stored on internal network servers. Even better would be to use a removable hard drive in this system and at the end of each day storing the hard drive deeper inside the physical perimeter and physically disconnecting the electrical access to the network.

Walls
Let's look next at the walls of your facility. The first question you should ask is "What material is it made of?" If you have properly secured the doors and windows of your building, an intruder may consider gaining entrance through a wall. If materials such as brick or cinderblock were used, then breaching an exterior wall will be more difficult than if stucco, vinyl siding, or glass (as is becoming more common in modern office buildings) were used.

If you're considering building a new facility, one option you might want to explore for your exterior walls (and some interior ones as well) is a construction technique called an Insulated Concrete Form (ICF) wall. Essentially an ICF wall is a standard metal or wood stud wall that has special polystyrene forms placed between the studs. The forms are then filled with concrete, which is allowed to set.

The ICF wall is usually touted as being much more energy efficient than a standard fiberglass filled wall [Reddi-Form]. It also provides an additional layer of defense against physical intrusion. While ICF walls may not be necessary for brick or cinderblock construction, they should at least be considered if the exterior wall material is either wood, stucco, or some other material that can be easily penetrated.

Roof

If you're in a multi-floor office building, you probably don't need to worry too much about your "roof". It will be the floor of the office above you. In most office buildings the ceiling above you (and the floor below you if you're not on the first floor) is actually reinforced concrete slab and will provide a reasonable amount of protection from physical intrusion.

If you're in a one-story building, or on the top floor of a multi-story building, however, your roof is another entry point for intruders. In addition to simply cutting through the roofing material, there are plenty of vents and ducts that could be used to gain entrance.

While you may not be able to use a stronger roofing material simply because of weight factors, you should still take precautions to prevent and detect intrusions from the top of your facility. Using alarm system components such as motion sensors and infrared "trip wires" in crawl spaces will help detect an intrusion through the roof. Security cameras should also be used to monitor and record any activity.

Vents

Any vents or openings in the exterior walls and roof of your facility large enough for a person to crawl through should have burglar bars welded across the inside of the opening. Directory of Central Intelligence Directive 1/21 (DCID 1/21) recommends that any opening with a cross sectional area of 96 square inches or greater be protected with one-half inch iron bars welded together and spaced every six inches [DCI, p. 13].

Barriers

If your ground floor walls consist primarily of floor to ceiling glass windows, you may want to consider the use of vehicle barricades to prevent intruders from ramming through the wall to gain access. You may have seen security camera footage of criminals backing a truck through the glass wall of a convenience store, load the ATM machine into the back, and drive off to later break into the ATM machine at leisure. The same strategy could be applied to gain access to your critical information resources.

If your risk assessment determines that vehicular ramming is a possibility and needs to be protected against, there are several possible ways to deal with this threat. The first is a concrete or steel bollard. This is simply a series of strong poles that stick up out of the ground and are spaced at regular intervals to prevent a vehicle from approaching a glass wall [Safety Line]. Other barriers include heavy planters that conceal a highway vehicle barrier to stop vehicles [Stonewear].

Another barrier option is a fence structure around the building. Modern fences for high security applications now include a fiber optic intrusion detection system [Fiber SenSys]. These systems can detect fence cutting and climbing. They work by detecting distortions in a light wave as it propagates through a fiber optic cable woven into the fence. Some fiber optic intrusion detection systems can also be used to detect glass breakage or are buried under grass, sand, or gravel to detect pedestrian and vehicular traffic [Fiber SenSys].

Access Control

Once the physical structure of your facility is as strong as it needs to be, you can then turn your attention to controlling normal day to day access into your facility. The basic principal here is to establish "zones" of security and only allow employees into areas they need to work in to accomplish their jobs. This "need-to-be-there" policy is similar to the "need-to-know" rule in controlling access to information. Don't grant someone access to an area if they don't need to be there.

Typical zones are the external perimeter, server rooms, wiring closets, classrooms, and various office spaces. Once your zones are established and a list of employees and their access requirements determined, you can examine what technologies you can employ to enforce your policy.

There are a wide range of products available and your selection depends on the level of risk to your facilities and information. Standard access control products include systems such as a keyed lock and a mechanical or electric combination lock [NoKey].

Medium security systems utilize a proximity radio frequency reader or magnetic card reader often combined with a personal identifying number to control access to a door. These systems are often wired back to a central control system so that multiple doors and zones can be controlled from a single location [Hirsch]. One recommendation I have is that the computer used to control your access control system not be connected to a network and should be stored in a location that is only accessible by authorized security personnel such as its own closet or a locked cabinet.

High security systems utilize biometric readers to control access. Biometrics utilizes physical characteristics of the person trying to gain access to identify them and determine if they are authorized access. Fingerprint recognition, iris recognition, hand geometry, and face recognition are some of the more common types of biometric systems in use.

Surveillance Cameras
After your barriers to physical entry have been placed, you still need a separate monitoring system to help determine when those barriers have been compromised. Security camera systems can be used to monitor high risk areas (doors, rooftops, exterior perimeters, and critical equipment) to provide a visual record of the intruder and the intrusion attempt for possible legal prosecution. Whether constantly monitored by security personnel or recorded on time loop tape, the visible presence of the security camera will act as a deterrent against intrusion and theft. deterrent

One thing to keep in mind when using security cameras is to ensure that every camera can be seen by at least one other camera. If you have one camera that is not monitored itself, that camera can be tampered with and disabled without the act being recorded. If one camera can be compromised, then the rest can be tampered with as well. While at first this seems to require a doubling of the number of cameras required, if the layout is well planned it may only require one or two extra cameras. Only remote cameras that don't have any others nearby will need an two cameras for each location. In this case, I would recommend that the main camera be visible while the backup camera (pin hole type camera) is well hidden.

A second tip with security cameras is to ensure the video tape recorder (VTR) is secure. If someone were to breach your physical security and in the process steal or destroy the tapes, then the purpose of the security camera system would be defeated. Only by locking the VTR and archived tapes in a secure room, closet, or equipment rack can you prevent the theft of the tapes. You may also want to consider using a second VTR in a different location, off site if possible, to have a backup of the surveillance camera video.

Alarms
A remotely monitored security alarm is a requirement for any business facility. A multi-zone alarm that can arm and disarm different zones independently lets you disarm your primary zone during office hours while still ensuring that less frequently used areas are still protected.

You may also want to consider using a "24 hour" alarm zone on areas that will be accessed very infrequently such as mechanical rooms or "emergency exit only" doors. A 24 hour alarm zone is one for which there is no way to disarm the sensors. If this area must be accessed, the monitoring company must be informed prior to entering this area and the identity of the caller verified so that an alarm response won't be initiated. This setup helps provide a higher level of security for often overlooked areas that can be used to gain access into your facility.

Alarm system components include door and window sensors, motion sensors, fire and smoke detectors, infrared "trip wire" sensors, and temperature sensors. The alarm system

components should be placed to ensure that each possible physical penetration point of the system is monitored.

Server Room Security

Now that the perimeter of your facility is secured, we can turn our attention to the interior of the building. We'll next examine the physical security aspects of the server room. This is the heart of your information system and must be appropriately protected. We'll begin much as we did with facility security and look first at "sealing" the room and then at ways to detect an intrusion attempt.

Doors
The doors of your server room should be at least as strong as the main perimeter doors, if not stronger. They should be of solid core construction, possibly with an outer steel covering.

Glass is a material to definitely avoid in server room doors. Even a small glass window could be broken and allow the door to be opened. Also, there should not be any glass sections adjacent to the door.

Walls
The walls of the server room need special attention. One problem commonly seen in office building server rooms is that the wall does not go all the way up to the true ceiling or down to the true floor. There is typically a gap of a foot or two above the false ceiling or below the raised floor. The problem with this is that someone in an adjoining room can gain access to the server room by simply climbing through the gap in the wall.

Another consideration is sound attenuation. If the walls of the server room are thin, then someone outside the server room could hear system administrators discussing sensitive information inside it. A common solution to this is to use fiberglass insulation inside the wall and a double layer of sheetrock on the exterior side of the wall. This will greatly reduce sounds from inside the server room reaching the outside.

The server room walls are an ideal place for employing insulated concrete form (ICF) construction. Having a wall of solid concrete surrounding a server room will provide very good protection from physical intrusion through the wall.

One final note on the server room walls is that they should not be external building walls. There should be a hallway or another room between the server room wall and the external facility wall. If the server room wall is an external facility wall, it should be of strong construction and not contain any windows or doors. If there are windows or doors leading from the outside directly into the server room, they should be permanently sealed to prevent an easy intrusion path directly into the server room.

Floor and Ceiling
The server room floors and ceiling shouldn't require any special attention if they are of solid construction. What must be watched, however, is the space above the false ceiling and below a raised floor. These areas are usually filled with electrical and data cabling and it would be easy for someone to tap into both and hide equipment in these areas.

A good security administrator will know what every cable is for in these areas and regularly inspect them for any extraneous cables or devices.

Access Control
Even if you only use keys for the rest of your facility, you should have an electronic access control system for your server room. Logging who enters and leaves this room is a must. If anything were to happen to the systems in here, you need to be able to determine who the last few people in this room were.

Alarms
Your server room should be a separate alarm zone. This way you can have it alarmed even during normal business hours. Only when authorized personnel are in the server room should the alarm for this area be turned off.

Vents
Any vents or openings in the wall of the server room that are large enough for someone to climb through should be sealed with burglar bars similar to the recommendations in the facility vent section above. This includes any openings in the walls for cable trays, which are usually quite large.

Racks
The equipment racks in the server room should be constructed of heavy gauge steel or aluminum and locked at all times. A locked key cabinet can be located inside the server room for storing keys to the racks and equipment. This way the administrators only have to have possession of a key to the key cabinet.

In large server rooms with many locks, not everyone should have access to all the equipment racks. A system such as the Electronic Key Tracker [KeyTracker] can be used to allow individuals access to only certain keys in the cabinet. This will prevent someone who has access to the server room from gaining access to racks of equipment which their job function doesn't involve.

Servers
Servers themselves need to be protected against physical intrusion. Here are a few suggestions:

- Use power switches that are lock controlled.
- Remove unneeded floppy and CD-ROM drives.
- Add a media lock to required external drives [SecureServices].

- Replace standard screws on servers with ones that require a special tool to remove.
- Use locking screws to mount equipment in the racks.
- Use a clamp on the server power cord to prevent removal.
- Use a BIOS password on the server.
- Check for hardware keystroke loggers [KeyGhost]. These can also be located inside the keyboard. A small amount of wax on the keyboard screws will serve as a visual indicator of tampering.

These recommendations will provide a final layer of deterrence to anyone who has managed to penetrate your other physical defenses.

Equipment Security

Now that we've looked at the external perimeter of your facility and the heart of your network, the server room, let's turn our attention to the rest of the equipment in your building. If someone, particularly an employee, can get into your facility but not your server room, the remaining equipment is likely to be their target.

Wiring Closets
The wiring closet is susceptible to attack because it is usually not very well protected, is not often checked, and has lots of connections to lots of systems. The destruction of equipment is one threat in a wiring closet. Another threat is that a small packet sniffer can be easily hidden in a wiring closet.

Most of the same considerations for the server room apply to wiring closets. You need to ensure that the walls of the wiring closet go from true floor to true ceiling, that all vents and openings are sealed, and that the door is resistant to unauthorized opening. If possible, use an electronic access control on wiring closet door and alarm the closet, possibly with a 24 hour alarm.

Cabling
Cabling outside of your server room needs to be considered a target as well. The two most common threats are cutting and tapping.

If all computers are networked via switches, then the risk to most cables is minimal. You do need to consider protection for cables that connect high value systems. Examples would be the cable that connects the company officers' computers to the network, any workgroup server cables, and inter-switch links.

The most common way to protect selected cables is to use steel conduit from one end to the other and run the cable through the conduit. The conduit will protect the cable from tampering and will provide visual evidence of tampering. If you use conduit, be sure to include them in your regular physical inspections.

Computers
The computers that employees use on a day to day basis are another resource that needs to be protected. Although the price of the hardware itself isn't trivial, the information stored on that hardware is much more valuable.

You can protect your systems from theft by using locking cables that attach in various ways to the case. For more security you can use removable hard drives and store the drives in a safe when not in use. You also need to inspect them for keystroke loggers.

To protect against using a bootable disk to bypass file access controls, remove floppy drives or use a media lock, change the boot order in BIOS so that the hard drive boots first, and use a BIOS password.

For laptops, you should consider using encryption for sensitive files. The Encrypting File System that comes with Windows 2000 and XP should suffice for some applications. Other third-party products for encrypting files include PC Guardian's Encryption Plus Hard Drive [PCGuardian].

Additionally, if a laptop is stolen, you might be able to recover it if you're using a product such as Stealth Signal [StealthSignal]. This software sends a message to the monitoring site every time the laptop connects to the Internet. If your laptop is stolen, the messages can help law enforcement track down and possibly recover the laptop.

Media Security

One last item remains to be secured. That is the removable media that information is stored on. This includes floppy disks, ZIP disks, tape cartridges, CD-R disks, and CD-RW disks. Newer media such as flash memory cards, IBM micro drives, and USB key fobs are also becoming popular storage options.

The two threats here are that information on these media can be compromised if not properly destroyed or that removable media can be used to make copies of files and secretly take them from the premises.

One way to reduce the threat from removable media is to implement a tracking system. All removable media should be given a serial number when it is purchased. You can then use a database to track who the media was given to, when it was returned, and when it was destroyed.

It will still be difficult to prevent users from bringing in their own media. By posting notices that bringing in your own disks is not allowed and that doing so will subject you to possible termination, you can let employees know you are serious about your information security. It won't be fool proof, but removable media is one of the weakest

links in the security chain when considering the insider who wants to steal your information.

The other way to reduce the threat of removable media is to properly destroy it when you no longer need it. There are three types of removable media: magnetic, optical, and electronic. Electronic media can be destroyed by a pair of pliers or a hammer. Take the case apart using a small screwdriver to get to the memory chip itself and then break the chip into several small pieces. Try to expose the silicon core of the chip and break it as well.

Optical media is expensive to properly destroy. A CD grinder is the best option to destroy optical media [Whitaker], but can cost several thousand dollars. These devices grind the data layer into a fine dust that makes it impossible to reconstruct. Another method is to use a belt sander. While this is less expensive, care must be taken to prevent injury.

I would not recommend any other method such as burning, microwaving, or breaking. Burning or microwaving a CD will produce toxic fumes. Breaking the disk may cause cuts and the pieces could possibly be reconstructed.

Magnetic media is easily erased by a bulk eraser [Whitaker]. By placing the media in the strong magnetic field the data is erased. Again, burning the media is not recommended because of the toxic fumes produced.

Conclusion

We've looked at many recommendations for enhancing your physical security. Depending on your situation, you probably won't need to implement all of them. The first step must always be to perform a risk analysis to determine what the most likely threats are to your information systems. Once you know the threats, you can plan your defenses appropriately.

Physical security alone won't prevent your network from being compromised. It will, however, complement any other network defenses you have in place. As a very determined intruder is thwarted by your virtual defenses, they may very well start looking for holes in your physical defenses.

References

[DCI] Director of Central Intelligence. *Directive 1/21: Physical Security Standards for SCI Facilities*. July 29, 1994. PDF Document on Web Site.
URL: http://www.fas.org/irp/offdocs/dcid1-21.pdf (Verified: May 20, 2002)

[Fiber SenSys] Fiber SenSys, Inc. *Fiber Optic Perimeter Security & Intrusion Detection.* Web Site.
URL: http://www.fibersensys.com/ (Verified: May 21, 2002)

[Hirsch] Hirsch Electronics, Inc. Web Site.
URL: http://www.hirschelectronics.com/ (Verified: May 21, 2002)

[KeyGhost] Key Ghost Ltd. Web Site
URL: http://www.keyghost.com/ (Verified: May 24, 2002)

[KeyTracker] Key Tracker Ltd. Web Site.
URL: http://www.keytracker.com/ (Verified: May 21, 2002)

[NoKey] The Keyless Lock Store. Web Site
URL: http://www.nokey.com/ (Verified: May 21, 2002)

[PCGuardian] PC Guardian, Inc. *Encryption Plus Hard Drive*. Web Site.
URL: http://www.pcguardian.com/software/hard_disk.html (Verified: May 24, 2002)

[Reddi-Form] Reddi-Form, Inc. *Insulating Concrete Form Construction*. Web Site.
URL: http://www.reddiform.com/ (Verified: May 20, 2002)

[Safety Line] Safety Line, Inc. Web Site.
URL: http://www.safetyline.com.au/centurian__fixed_bollard.htm
(Verified: May 21, 2002)

[SecureServices] Secure System Services. *Media Drive Lock*. Web Site.
URL: http://www.secureservices.com/ds/66132s.html (Verified: May 24, 2002)

[SecureTech] SecureTech Solutions, Inc. Web Site.
URL: http://www.securetech.com/ (Verified: May 21, 2002)

[StealthSignal] Computer Security Products, Inc. Web Site.
URL: http://www.computersecurity.com/stealth/index.html (Verified: May 24, 2002)

[Stonewear] Stonewear Force Protection. Web Site.
URL: http://www.planterbarrier.com/ (Verified: May 20, 2002)

[Whitaker] Whitaker Brothers. Web Site.
URL: http://www.whitakerbrothers.com/federal/prod_com_spmedia1.asp
(Verified: May 25, 2002)

Last Updated: May 25th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event