Global Information Assurance Certification Paper

Joshua Sukol
May 2, 2004
GIAC Security Essentials Certification (GSEC)
Practical Assignment Version 1.4b, Option 1

Providing Physical Security for Digital Assets

(Protection on the Tangible Perimeter)

Abstract
Effective Information Security implementations follow the discipline of defense in depth. One of the many areas that need to be addressed to provide proper security for every organizations security needs is Physical Security. Without a properly implemented Physical Security Program your organization will have a gaping hole for intruders to attack. If an intruder gains physical access to a workstation or network device it can have devastating effects.

The focus of this paper will be on providing an overview of how to approach physical security planning so that you can properly mitigate risks. This paper will not go into depth about designing building structures or creating data center security implementations, but those issues do come up briefly in the overall process. What we will focus on is an overview of how to apply physical security to match your organizations workflow and security needs. This paper will also discuss techniques for mitigating risks that your organization may face. Every organization is different and structured in a different manner, however the information presented in this paper can be adjusted to fit just about any organization that has multiple departments and a definable workflow.

Defining the Non-Digital Perimeter
Security is all about control. Through Physical Security Policy and employee awareness you must develop a program that dictates control of your physical environment if you are going to provide security for your digital assets. You should begin by defining your organizations areas of operations to allow you to begin creating zones. The purpose of establishing zones is so that you can define standards for them and place the appropriate controls on them. Defining the zones allows you to begin segregating your organizations functions, as well as the actual physical boundaries. It is important to develop zones early on the process because part of the risks that a zone might face will come from another zone that has an entry point into that zone. In the document "Physical Security Standard" [1], which is published on the Treasury Board of Canada website, zones are defined into the following categories:

- Public Zone
- Reception Zone
- Operations Zone
- Security Zone
- High Security Zone

The intent of that document is to describe and outline physical security standards for government buildings. The same model, however, is adaptable for use by many different types of organizations and businesses. I have defined the zones mentioned above somewhat generically so they can be applied to multiple business atmospheres.

Zone Definitions:

Public Zone:	This is the area around your building or office space that is open to the public. This could be the hallway in an office building with multiple tenants, the parking area, or other grounds around your building that are accessible to the general public.
Reception Zone:	This is the area where visitors, customers, or employees first enter the physical perimeter of your organization. Keep in mind that you might have multiple reception zones depending on how large your area of operations is. Also, reception zones are not just areas where you greet visitors. This type of zone would be referring to basically any entrance to your facility. Some examples of reception zones that might be overlooked are shipping and receiving areas, and employee entrances.
Operations Zone:	This is the area where office workers are located. Multiple departments might be included in the operation zone, however when you begin auditing they must be separated on paper if they have different security needs since the access controls will be different. This area is also the most common area where visitors, or clients might be meeting with employees of the organization. When in this area all non-employees should be accompanied by an employee escort at all times.
Security Zone:	This area would be an area that is restricted to specific personnel. Generally there would be additional authorization required to be in this area. Additional access controls would also be implemented to provide the proper security for this area. Visitors accessing this area would not only have to be authorized themselves, but they would also have to be escorted by authorized personnel. This area most likely will not be accessible from outside the building. The access would come from within the operations zone.
High Security Zone:	This zone is similar to the Security Zone but it would have more stringent access controls.

Broad Mitigation Techniques

The purpose of this section is to introduce you to some of the physical security concepts that will be applied to each zone and your organization as a whole. The concepts of these controls can be applied to almost any organization, however the level of complexity to which you implement them will depend on the needs of your organization. When you are designing a physical security plan you need to be aware if the industry you are working in requires the need to meet compliance regulations. Compliance regulations could very well dictate the types of controls that you will need to implement. Two primary examples of this are the Gramm Leach Bliley Act (GLBA) regulations that apply to Financial Institutions, and the Health Insurance Portability and Accountability Act (HIPAA) that apply to a variety of different companies that keep or store medical records.

The Public Zone

Closed Circuit Television (CCTV) can increase security at any entry point throughout your organization, but it is of significant use in the public zone because it allows security guards (if the closed circuits are actively monitored) to monitor threats that might be moving towards your area. If the video feed is recorded it can also provide visual documentation in the event of a robbery, vandalism to your property, or other types of incidents that may occur in the area that is being monitored. If the cameras are visible to people in the public area they will also act as a deterrent.

Designing or modifying the public area with physical security in mind is another way that organizations can add layers of defense. For example, clearly marked boundaries and well lit up parking areas allow guards on duty to easily identify when the perimeter has been breached. In addition, proper security lighting is necessary for CCTV cameras to be effective. (Treasury Board of Canada, Physical Security Standard)

Reception Zone

If your organization services a lot of clients or customers onsite, has a lot of visitors come to your building, or has a large number of employees this area or these areas will most likely see a lot of traffic pass through. You can begin providing security to this area by implementing CCTV at your entry point. As discussed earlier this is an effective deterrent as well as an effective tool for providing visual documentation and evidence. If you are servicing customers in a retail environment you most likely will not want to ask them to sign in. However if you are servicing customers in non-retail transactions or the person is a visitor coming onsite for a meeting you may incorporate this into your physical security program. This technique is used to provide logs of who has gone in and out of the building. Depending on your circumstance you may require photo identification or another form of ID before logging someone in. For employees and vendors it is common for larger organizations to handout ID cards that are required to be shown before access past the reception zone is permitted. In addition you might need to define areas in the reception zone that are off limits to

unauthorized personnel such as retail counters, or the receptionists desk. These areas should be clearly marked and have some type of barrier separating them from the general reception area. Visitor badges can be given at this point as well. It might be intrusive to give visitor badges in certain situations but it is a good practice if it can be performed in an un-obtrusive way. This is especially important for organizations with lots of traffic in and out of the building. It is much easier for office personnel as well as security personnel to spot an intruder if they are not wearing a visitor badge when they should be, or if they are wearing a visitor badge and they are in an area that they should not be in. This technique is most effective in large organizations where all people onsite are required to wear either an employee or a visitor badge. Some organizations may find it necessary to color code visitor badges so that you can easily identify what levels of clearance a visitor has been authorized. This will help to prevent employees from escorting guests to areas where they are not permitted. Although there is the possibility of visitors receiving false badges from an employee it is still a good practice to require them. In order for it to work effectively you should implement a policy that the person escorting the visitor cannot be the person who assigned the visitor badge. This will setup a system of dual control as long as the policy is followed properly. Keep in mind that many reception areas will be the common area for all visitors entering the building. This makes your risk for theft and exposure to unauthorized access much higher. Physical securing equipment and providing increased protection standards is necessary to protect devices in this area. Techniques that could be used are things such as physically securing the computers to desks, or making use of thin clients so that in the event that theft occurs you will not be losing data that might be stored on the computer itself.

Another technique that is most effective in large organizations or organizations that require a high level of security is to extend the perimeter as far from the building as possible. An example of this would be if fencing surrounded the entire property and the entrances were gated manned guard stations. This would move the initial reception zone before the parking lot. This will allow security personnel to monitor all car and foot traffic entering and leaving the property. This would give the guards a chance to stop individuals and gather information such as license plate numbers, the purpose of the visit, and the expected duration of the visit. Guard personnel could then keep records and notify other security personnel throughout the property if necessary.

Regardless of your individual situation it is vital that you have well documented procedures for how customers, visitors and employees are treated when entering this area. You must strike a balance between providing security for your organization and a friendly reception area for visitors and customers. A well-written policy and proper training of your employees will ensure that security objectives are met and that this layer of security is effective.

Operations Zone
The operations zone will most likely be the center of high activity for your organization. Different types of operational zones could include things like the accounting department, administration department, human resource department or something like a call center. It is not uncommon in many companies to have meeting areas in operation zones where representatives of your company from their respective departments meet with visitors on a regular basis. It may even be that multiple departments have a need for their own individual area to meet with visitors. When defining your physical layout try to keep these meeting areas removed from the heart of the operational zone in which they are located. In this case well-documented rules are also necessary so that employees that work in these areas as well as the employees escorting guests know where visitors should and should not be. If at all possible it would be a good practice to separate meeting areas from operation zones with an entry point such as a locked doorway. Because of the increased threat of outside access to confidential company data by having visitors on site, well-defined practices should be implemented regarding the safeguarding of electronic and paper information. If possible meeting areas should be devoid of computers and networking equipment as well as paper documents that contain information un-related to the meeting taking place. Extra care should be given to the placement of network jacks and wiring that might run around, through, or over meeting areas. The data that is potentially available and the physical threats to equipment must be properly identified in each department or operational zone so that the proper mitigation techniques can be implemented. Where Management deems necessary additional entry points should block access from one operational zone to another.

Security Zone
Any area that is defined as a security zone would most likely be an area that is used for storing confidential data, or possibly a server, or data center area. It could also be a lab that needs to be kept secure to prevent contamination of experiments, or possibly private research is done in this area. Regardless of what is happening in your security zone this is a zone that requires more stringent control. It could be as simple as a locked door that only authorized personnel have keys for, or it could be as complex as biometric systems that control access via retina scans or fingerprint scans. Defining appropriate controls really depends on the needs of your organization, and how much management is willing to, spend. The best way to make a case for funding is to provide management with threat analysis of the types of data that are stored in these areas and the potential effects that disclosure of that information could have.

High Security Zones
This zone is very similar to the security zone but it requires an even more stringent set of access controls. This type of zone would be used to define areas that require the highest level of security. In most cases they will also be the

areas that have the least amount of employees needing access. In some situations a high security zone might call for additional monitoring equipment, possibly additional guards to protect entry points, and most likely additional written policies and procedures that apply to the personnel using this area.

Threat Assessments & Auditing Techniques

Now that a set of zones have been defined and broken down into individual departments you need to properly identify the threats that are in each area. It is out of the scope of this paper to define auditing techniques, however a discussion on the topic of auditing is included along with some references to give an idea of what needs to be done in order to effectively audit your physical environment.

Many threats are general to the entire organization but need to be approached differently in different zones because of access concerns for employees to be able to efficiently do their daily tasks. In addition zones that are further removed from the public zone and the operational zones may allow activities that would not otherwise be tolerated. For example, a workstation that is setup in a security zone might not need to be bolted to a desk while a workstation in the reception area would most likely require it. Keep in mind though that this is only acceptable if proper security techniques are implemented from the very beginning. If just about anyone can walk into the security zone this statement would not be true. Of course if just about anyone can gain access to the security zone you have a lot of work to do before you can begin to have an effective level of physical security.

Assessing Risk

According to the Audit - IT Examination Hand book available on the Federal Financial Institutions Examination Council Website[2] *An effective risk-based auditing program will cover all of an institutions major activities.*
Although that document is geared toward defining requirements for auditing financial institutions the message is clear. In order to adequately assess the risks associated with the target of your assessment you must be thorough.

The most general risk for all institutions is unauthorized access. Unauthorized access is access to anything within the organization that the individual should not have access to. This includes paper files as well as workstations, and networking equipment. In previous sections of this paper we have already discussed the concepts of setting up physical access controls for your building. The focus of auditing is to identify the potential risks that reside in each zone. A good foundation for this process can be found in the FFIEC Information Technology Examination Handbook.[3] Below are some direct excerpts from the handbook. These excerpts come from a section titled “Information Gathering”.

- *Obtaining listings of information system assets (e.g., data, software, and hardware). Inventories on a device-by-device basis can be helpful in risk*

assessment as well as risk mitigation. Inventories should consider whether data resides in house or at a TSP.

- *Determining threats to those assets, resulting from people with malicious intent,7 employees and others who accidentally cause damage, and environmental problems that are outside the control of the organization (e.g., natural disasters, failures of interdependent infrastructures such as power, telecommunications, etc.).*

- *Identifying organizational vulnerabilities (e.g., weak senior management support, ineffective training, inadequate expertise or resource allocation, and inadequate policies, standards, or procedures).*

- *Identifying technical vulnerabilities (e.g., vulnerabilities in hardware and software, configurations of hosts, networks, workstations, and remote access).*

- *Documenting current controls and security processes, including both information technology and physical security.*

- *Identifying security requirements and considerations (e.g., GLBA).*

- *Maintaining the risk assessment process requires institutions to review and update their risk assessment at least once a year, or more frequently in response to material changes in any of the six actions above.*

These "Information Gathering" steps are directed at compliance for Financial Institutions but they provide the proper grounding to begin auditing in just about any environment. Depending on your organizations needs you may decide to implement a full blown audit of your entire organization, or you may already have an audit that you can extract information from that is relevant to this physical security audit, or you may feel the need to audit physical security independently of other audits. Whatever format you use to audit your environment be sure to be thorough and properly identify risks.

Common Risks and Mitigation Techniques

Once you have completed your audit you should have a list of your vulnerabilities, and a list of what controls are currently in place to protect them. As you start to go through the list to determine if the controls in place are adequate you will likely find some very common themes throughout your entire organization if you have not already been through this process before. Below are some of the more common vulnerabilities that you may come across. If you do not pick these types of issues up during your audit you may need to go back and do some additional field work, unless you are auditing a second time after the mitigation techniques have been implemented.

Inadequate Access Controls

Chances are this is going to be the area that you will spend the most time implementing corrective controls. Many organizations have not implemented zones and therefore do not have proper controls to restrict access to physical areas of the building. In a larger office it makes sense to have key card access or push button codes to move from department to department. In offices that are dealing with more sensitive data it would not be uncommon to have entry points into different departments and zones that make use of retina scanners or finger printing devices. In smaller office settings you may find that an area such as your file room is not controlled properly and you may be able to mitigate the risks properly by using a series of keys that you only hand out to authorized personnel. The limit on how complex you are going to get is based on the size of your budget and the potential threat that you face in the event of unauthorized access. In terms of protecting your physical network environment you should pay special attention to the placement of your networking devices such as switches, hubs, servers, Intrusion Detection System (IDS), and Data Line Termination end points. These devices are some of the most critical components and should receive the most attention. Many organizations put these types of devices in closets, common storage areas, and sometimes in a users office. In the wrong hands they can be easily compromised in less than a few minutes.

Removable Drives

CD-Rom Drives and floppy drives are the most common removable drives that you will find. These drives pose a security risk because of the potential for an attacker to use them to boot into an alternate operating system. Once in the alternate operating system they can use password-cracking tools to gain administrative access on that computer, or they can boot into another system and mount the local hard drive giving them access to read and write files. These types of drives could also be use to introduce viruses or malicious software onto the network. A good practice for mitigating this threat is to remove all drives that support removable media if it is not required for that workstation. In a typical business environment CD-Rom Drives are primarily used for installing applications or for receiving large files from outside your organization. In most cases you do not want end users to have the ability to install applications anyway. With the amount of protection that you gain by removing the drives it is worth the aggravation to force users who receive files on a CD to fill out a request form to give to the IT Department or Help Desk along with the CD requesting to have it loaded onto the shared network. Floppy drives should be treated in the same manner. The number of users who actually have a legitimate need for a floppy drive is most likely very low. In most cases removing it will probably have an acceptable negative impact on the workflow in your organization. In some cases you will run into users who do have a legitimate reason to keep their CD-ROM drives. A good example would be if you have a graphics art department. Graphics designers are often working with other vendors and receiving large files. If they were forced to fill out a form and wait for a tech to load their files every time the received a CD they would most likely not

be very productive. In a situation like that I would recommend concentrating on other mitigation techniques. It may make sense to require a standard key to get into their office or something like a magnetic keycard. However, you must make sure that policy dictates that they are not to leave the door open or allow other users to access their workstations. A well-written policy will state that it is against company policy to attempt to circumvent access controls, and this scenario should be one of the examples.

Rogue Network Ports

How many network drops do you have on your network? How many of them are in use? How many of them are cross connected on your hubs or switches? The point here is that you need to know the answer to all of the above. It would not take long for an intruder to plug in a laptop and make use of a network sniffer to gather passwords, or other data. Imagine the effects it could have long term if for some reason there was a network jack that was left active in closet where a computer would not be noticed for days. An attacker could leave a computer running an enterprise wide vulnerability scan and come back to get it days later. Other than users who take their laptops home with them, or conference rooms where users meet and have a need for a live network jacks in order to give presentations, there are not many uses for leaving empty jacks cross-connected. Of course it is one more thing to remember when someone moves offices, or when a printer moves to a different shared area, but the level of security that you gain by disconnecting network ports is well worth the effort. If for some reason you do leave empty jacks active you should at least have another control to help decrease the area of exposure.

DHCP & Port Control

DHCP does not really fall into the category of physical security by itself, but it can come back to haunt you during a physical assessment. As your walking around diligently checking to make sure that your network jacks that aren't in use have been disconnected you may find one that has been missed. Your dutiful DHCP server offers you up an IP Address so that you can begin hacking the network faster. In addition to giving you an IP Address the server will most likely give you the IP address of at least one and possibly two DNS servers. It will provide the default gateway. If you are using WINS it may even give out addresses for WINS servers, and in addition it will probably provide the fully qualified domain name of the internal network. With all of that an attacker has plenty of information to begin probing your network for a good place to begin an attack.

Many modern switches offer you the ability to use mac-address control on each of its ports. Locking down switches can become a lot of work for you, and mac-addresses can be spoofed, but security is about control and layers of defense. By disbabling DHCP, and locking down your switches to only speak with known mac-addresses you provide security for the physical connection to the network. This issue is not just about unused ports either. If an attacker gains access to

any office in your building he could easily unplug a desktop pc and plug in his own.

Paper File Sensitivity
Many people find it easier to audit network devices and computer settings from printouts rather than working from the monitor. Your employees need to understand that print outs, and file dumps retain their sensitivity even after their usefulness expires. In the hands of an experienced hacker a printout of your firewall settings can be as detrimental as if they had gained physical access to the firewall itself. This risk does not just fall into the IT Department either. If an attacker begins reconnaissance for an attack by dumpster diving and finds a copy of the un-shredded document he was after before his technical attack even begins it would not matter what other security measures you had in place.

Protection Against Theft & Physical System Modification
Even with many layers of protection in place you are still vulnerable to loss of data or system compromise if an attacker can walk out the front door with one of your computers. If the attacker is not that brazen he might just remove a hard disk and carry that out in his pocket. Some techniques to mitigate that type of risk include physically securing the computers with cable locks, encasing the computer behind some kind of door or locking cabinet, or using locking screws that require a key or a special tool for removal. These techniques may not be one hundred percent fool proof but they do act as a deterrent and will increase the amount of time it takes for an attacker to compromise your system(s). Another good technique that can be used is to require a signed authorization form for removing equipment from the building. This will only be effective if you have someone monitoring exit points from within your security zone or your building. In a highly secured environment you implement a policy that does not allow employees to bring purses, or bags onsite. Again this is not fool proof, but it can help to prevent casual theft of company data or materials.

Sticky Notes
Many security audits will undoubtedly turn up notes with usernames and passwords written down in users work areas. Common places to look for these are taped to the bottom of keyboards, in desk drawers, and sometimes they are in plain site taped to monitors or on corkboards. The only way to combat this is to write policy that states that this practice is unacceptable. In addition random checks for these types of notes can be effective if you follow it up by formally reprimanding users who do not comply with the policy.

Defining the Attacker
To this point we have been discussing protecting your network from “The Attacker”. It is important to understand that these techniques and controls apply to employees within your organization as well. In fact it has been reported that insiders perform 80% of attacks on network systems[4]. What this means is that in

most cases it is one of your own employees who is performing the attack on your systems. I have brought this up many times already but I cannot stress enough how important it is to have well written policies that dictate acceptable behavior and what your company policies are. In addition to that it is critical that your employees are trained to understand why the policies have been created. By increasing security awareness throughout your organization you are also increasing the chances that your honest employees will report suspicious or malicious activity.

Additional Areas of Concern

Providing physical security does not begin and end with developing and implementing security zones and personnel policy. In this section you will find an overview of some additional topics that should be considered.

The Physical Area

The geographical region that your company is in can play a role in choosing a location for your building. You must take into account things such as earthquakes, floods, fires, and other natural disasters. You will not be able to avoid all of the risks associated with these things, but you should take them into account when purchasing, or building your office space. If you are in an area that is prone to any of these types of disasters you should make sure that your building is designed in such a way that you will be protected as much as possible. Adequate insurance may leverage the potential for financial loss, but it will not help you to serve your customers if your data center is destroyed by an earthquake or submerged in water during a tropical storm.

Be sure that the necessary precautions are taken to ensure the most uptime and availability of your information services. It is a good practice for organizations to have a Business Recovery Plan that allows resumption in the event of a major disaster. The scope of your individual plan should correspond to the potential of threats and the financial loss associated with the unavailability of your information systems and business as a whole.

Electrical Power Concerns

Computer and networking equipment is useless if you don't have power to run it. Electrical, brown outs, spikes, and surges are potential risks for your desktop and data center environments. You can properly protect your self by using Battery Backup Systems to ensure that your systems stay running in the event of a power outage. In addition, certain types of battery systems will also serve as a protection against brown outs, spikes and surges. Generators can be used to provide ongoing electricity in the event that a blackout occurs for more than a few minutes.

Fire Suppression

In the event of a fire it is very important to have fire suppression available and working properly. Sprinkler systems are very common and useful throughout

your organization, however they can be very damaging in certain environments. Dousing your servers with water could potentially have the same effect to your business recovery plan as letting them burn with the building. It would also be extremely frustrating if the sprinkler system malfunctioned in your server room and doused your servers when there was not actually a fire. In the case of server rooms and other areas where water is more damaging than helpful you can implement chemical fire suppression systems such as Halon. Halon is effective in smothering fires by using a chemical reaction that eliminates oxygen in a room. This is obviously hazardous to humans so its use must be preceded by an evacuation.[5] In addition it is a good practice to have fire extinguishers throughout your building. In order for them to be effective employees need to be trained in how to use them and they need to be made aware of where they are located.

Shared Building Concerns

For many businesses it is unavoidable that you will be sharing a building with other tenants. When assessing your physical security be sure to take into account the fact that you might be sharing walls, heating ducts or raised floors with your neighbors. A wall that is easy to break through or that does not extend all the way to the floor or ceiling can become an additional entrance into your area in the same way that heating / cooling ducts can be. It may be necessary for additional construction to mitigate these risks.

Even if heating and air conditioning ducts are not big enough for intruders they may carry sound. In the event that they are located in a private meeting room your confidential conversations could potentially be heard in other areas of the building. In this case it may be necessary to install sound dampening material or remove the ducts all together.

High Tech Hacking

In some scenarios companies might have to worry about such high tech scenarios such as attackers monitoring electronic emissions from their computer equipment. These emissions are known as TEMPEST. There is paper titled "Protect Your Self" written by Justin Bois[6] available in the SANS Reading Room that explores this topic in greater depth. What this paper describes is how an attacker can monitor these emissions and view what users and systems are doing remotely. There are options for protecting yourself against these types of attacks but they involve special building materials or other high tech equipment that is used to muffle the signals. What this means in terms of designing security program is that you need to start thinking about security as early on as possible. If you have the luxury of designing your own building or at least the inside structure of your building you can design your plan to account for these types of attacks. Doing so will greatly increase your chances of avoiding costly building modifications and construction down the road.

Bringing It All Together

The topic of physical security is very broad and it is only one step in providing a security solution for your enterprise. Throughout this paper I made references to security policies and user awareness training. Those two topics will make or break almost every aspect of your entire security program. The other key step that you need to do well in order for your security program to be successful is auditing. You must know what you are protecting and what the risks are in order to successfully protect your organization. Be thorough in your assessment and implementation process, and don't to forget to revisit the topic of physical security as often as your environment calls for, and especially when there is a change in your physical structure or office space.

References

[1] Treasury Board of Canada. "Physical Security Standard."
http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/CHAPT2_2_e.asp

[2]Federal Financial Institutions Examination Council. "Audit – IT Examination Handbook" August 2003
http://www.ffiec.gov/ffiecinfobase/booklets/audit/audit.pdf

[3] Federal Financial Institutions Examination Council. "Information Security" December 2002
http://www.ffiec.gov/ffiecinfobase/booklets/information_secruity/information_security.pdf

[4]Intergov International Website. "Latest Web Statistics"
http://www.intergov.org/public_information/general_information/latest_web_stats.html

[5]Cole, Eric – Fossen, Jason – Northcutt, Stephen – Pomeranz, Hal. "SANS Security Essential With CISSP CBK Ver. 2.1 Volume 1" SANS Press. April 2003. 265-266

[6]Bois, Justin. "Protect Yourself" April 4, 2002
http://www.sans.org/rr/papers/43/271.pdf

Hsiao, Aron. "Teach Yourself Linux Security In 24 Hours 1st Edition. SAMS. Apr 13, 2001

Bragg, Roberta. "CISSP Certified Information Systems Professional Training Guide" Que Publishing November 2002. 529-570