The Other Physical Layer: Physical Security
GSEC Practical 1.3
Bret Jenkins
18 March 2002

Summary

Very often, when discussing network/systems security many IT professionals will overlook physical security. Applying hot-fixes and patches, running the many system security checklists available is only half the equation. To fully secure a network and its systems also requires a layer of physical security. Without it, we are vulnerable to accidental as well as malicious attacks that can affect our data. Protecting our data is the ultimate goal. By being aware of the often-overlooked physical security aspects of “who”, “what” and “how” we add that extra layer of protection through plans and policies.

Physical Security

I recently responded to an incident at one of my company’s data centers. Our help desk contacted me and explained that they could not contact one of “my” servers. After a bit of over-the-phone troubleshooting, we found that they could not contact *any* of the systems located at this particular data center. I immediately diagnosed this as a bad thing and drove carefully to this particular data center. Hoping it was “just” a simple network issue I walked into the data center and was surprised to see that the racks of normally active monitors, storage systems and NT/Solaris/Linux servers were dead. The only activity was a group of managers trying to figure out what had happened and a frantic electrician trying to determine why he could not get power into the room. (More on this later…)

As security professionals, we tend to concentrate on the technical or “cool” side of systems hardening. Thousands, even millions of dollars can be spent in man-hours, software and hardware securing our data. We spend countless hours locking down operating systems and applying hot fixes and security patches. But how much thought or resources do you put into the physical security of your equipment and infrastructure? Many of the books and papers on systems security will acknowledge the need for adequate physical security, but only gloss over the implementation. Take a look at this link: http://csrc.nist.gov/fasp. Note that out of all the best practices outlined on this site, there is only one high level document on actual physical security. Now, in their defense, physical security would require a book to effectively cover the subject and all the possibilities, but the subject of physical security is vitally important to properly securing your data. Properly implemented, a good physical security plan will help protect your systems from benign as well as malicious activity. Physical security is not however, another term for disaster preparedness. Many of the physical security solutions will fall into both areas, but the two should be considered two distinct areas. Fact of the matter is, if I have physical access to your systems and infrastructure, I have your bottom line in the palm of my hand. Unless you are in business just for the fun of it, I would say this is a pretty scary thought.

The thought process behind designing an effective, practical physical security plan is identical to designing an effective systems security plan; we need to determine what, who and how.

What
This is really where you need to begin. In order to accurately plan the who and how, you must have an accurate account of what you are protecting. What are the critical components of your network? Most of us probably jump straight to the components we are directly and most often responsible for. This is fair enough but it is important to understand that the rest of the systems and infrastructure are just as vulnerable to malicious attack or simple carelessness. Obviously, many of these components are going to be beyond your scope but begin by listing the components that you are responsible for and their physical locations. List components such as servers, admin consoles, routers, switches, cabling, patch panels, UPS, backup generators, demarks etc. (Personally, I would even go as far as to identify circuit breakers but, as I said earlier, “more on this later”.) Finally, you need to categorize all the components on your list. I have 3 categories in which I place a component:

> Cat A – Component is vital. Component/data loss would cause excessive or catastrophic loss of time/money. Irreplaceable.
>
> Cat B – Component is important. Component/data loss would cause significant loss of time/money. Replaceable at great cost.
>
> Cat C – Component is replaceable. Loss would be inconvenient.

Before categorizing your servers, backup systems, storage subsystems etc, you have to go a little deeper. What information is contained on these systems and how important is it? Could you stand to lose the data for a period of time? Is it sensitive or valuable information? This is absolutely vital to determining how and to what lengths you plan to protect the system on which it resides.

Who
Who has or needs access to the systems and to what level? In the case of physical security, we need to know who has *physical* access to the components on your list. Depending on the complexity of your network, the answer to this question can become complex very quickly. Probably the easiest way to do this is to list a particular location and the components in that location. Then begin to

note who has access to that location. If this is a location with access to the public, note that. Don't forget the security or facilities personnel who may have access as well. Then list everyone who requires actual physical access to each of the components. Finally, identify who is directly responsible for each of the listed components. This should be the individual or individuals who ultimately determine who is allowed access to a particular component.

How

How do we prevent all the possible screw-ups, accidents or outright malicious behavior from taking down our expensive systems? Fact is that you can't. That is you can't protect your system from *all* the possible combinations of what, who and when. What you can do is reduce the likelihood of any of the possible combinations affecting your systems. When discussing physical security, we do this by limiting access. The more important the resource, the more restrictive the access controls.

Outside Access control - How is access to the building controlled? You probably do not have control over this aspect but you do need to know. This can have a direct bearing on the plans and policies you do have control over.
One effective method of control is to have manned access points. It adds an excellent layer of security to your system but is only as good as the staff manning said access points. Another method involves using secure access points. This meaning a pass card , combination or key is required for entry to the building. Of the three, the weakest method is going to be combination locks. Where as it is relatively easy to maintain physical control of a pass card or key, it is impossible to control a combination except through policy. Policy may state that only authorized individuals have the entry combination but unless the penalties are rather severe (and management is willing to enforce it), it is quite easy for an employee to give the combination to someone who otherwise may not be authorized. In addition, many of the current cipher/combination locks used today offer others free view of the combination while being used. Unless shielded, it is not difficult for someone to casually watch while you input the combination.
Key locks offer good protection, however they generally have no means of tracking entry unless you use some sort of sign-in log. Even then, sign-in logs only account for people who take the time to sign in.
The most widely used method at this point in time seems to be the electronic pass cards. They offer good protection and allow monitoring and logging of access to the facility.

The biggest problem with combinations, keys and pass cards is lack of positive control. All these items can be lost. Unless the loss is discovered immediately, there is a window of opportunity that can be used against you. Another problem is cost and logistics. It may be relatively easy to disable and replace a pass-card but the process of re-keying a door lock or changing combinations can be expensive and time consuming. In a large organization, imagine the logistics involved in ensuring everyone has the new key or combination.

Gaining in popularity are the biometric access control devices. Just a few years ago, these were rather expensive. They have become much cheaper since then and are certainly worth looking into. No more pass-cards or keys to lose, no more combinations to forget and there is no doubt who is entering the facility. Barring KGB or CIA like resources, they are pretty difficult to circumvent in a *properly* designed facility.

Inside Access Control - How is access controlled to the various offices, rooms and closets that house your critical system components? This is where many organizations are the weakest. Great external security, but once inside, an individual has relatively unhindered access. At this point, we need to begin to look at the level of security each component requires. Is it a Cat A, B or C resource? Obviously, the more important the component, the more stringent the access requirements. All components should be secured behind locked doors using a combination, key or pass-card based system. Something as simple as key or combo lock and access lists are your cheapest alternatives but one thing to take into consideration is the logging feature a pass-card system offers. Depending on the sensitivity of the data, alarm and video systems may also be called for. Another thing to take into consideration when choosing a location for your more sensitive components, are alternative avenues of access. Make sure you don't spend time, money and resources securing the front door, only to find access possible through the ceiling tiles or under the false floor!

Power – How is power delivered to your systems? Are the circuit breakers located in a secure location? Are the circuits well marked to prevent accidental shutoff? Does your computer room have some sort of emergency power cutoff? If so, how likely is it that someone could inadvertently hit it? Consider using locking power plugs and receptacles for all your equipment. It is far too easy for someone to mistakenly or inadvertently unplug a component. By using a well marked locking power plug and receptacle, you can ensure that an accidental disconnect cannot occur.

Cabling – Is your critical cabling well marked? How vulnerable is it to damage? Is it easily accessible to the general population? Will it be used to transmit sensitive information? This includes not only your typical twisted pair and fiber cabling, but your wide area links as well. Consider using specific colors of cabling for critical links. At the very least identify them with tags at each end. This is especially important for your communications link. My company lost a T-1 link to our customer for nearly 4 hours after an installer disconnected our pair while installing service to another office. (His excuse was that he did not realize the pair was a live circuit.) To prevent inadvertent damage to cabling, use one of the several types of flexible conduit available. I have seen several instances of damage being done to cables already in place while new cabling was being installed. Conduit is simple, cheap insurance. Certain types of conduit when installed and used properly also act to deter data theft. Cables simply strung over dropped ceilings or otherwise accessible to the public are open opportunities for data theft. Imagine someone placing a wireless access point somewhere above your ceiling; a simple cut and crimp, and your data is now being broadcast out of your facility. Many security programs will require that cables used to transmit sensitive/classified information be enclosed in a hardened conduit and placed below any drop ceilings so as to be visually monitored.

Routers, switches, hubs, patch panels, etc. – Ideally, all these components should be placed behind locked doors. If that's not possible, consider placing all equipment accessible to the public in lockable racks that have been securely bolted into place. Bolting the racks into place prevents inadvertent movement of the rack which can damage cables or disconnect power. It's also just plain old safety and common sense; locking wheels will not prevent a rack full of equipment from tipping over. If only one thing in your system is considered a Cat A resource, it's you. Racks can also offer a certain amount of protection from fire, water and debris in the event of fire or disaster.

Servers and data storage systems – These are the center of our universe as we know it. Lock them up. Lock them behind closed doors then lock them in securely mounted storage racks. Power, mouse, keyboard and network cables should be securely mounted to prevent accidental damage or disconnection. Take the time to properly route the cables. I have accidentally pulled a power cable from a server while running cables to another server. Once you are satisfied they are securely locked up, begin to secure them individually. Ensure that servers cannot be booted from CD or floppy drives. This is usually done through the BIOS. Make sure to password protect the BIOS to prevent unauthorized changes to the settings. Use an external, real time monitoring and reporting system to alert you to any unscheduled outages. Also check your server logs for the same. Log checks are a very important part of any physical or network security plan. There are a few products available which, when given physical access to a servers bootable floppy or CD, will allow you to fully access the data on the drives. In order to use these products, an outage has to occur for a period of time. Using Winternals "Remote Recover" software and an NT Server as an example, I place a specially formatted floppy or cd-rom into a server and power it down. I connect a laptop to the server via a crossover cable to the network interface and then turn the server back on. Once the system has booted from the floppy or cd-rom, everything on that server is available to me. I grab what I need (the SAM perhaps), modify a few files, remove the floppy/cd-rom and turn the server back on. (By the way, don't make the mistake of assuming the "nix" operating systems are invulnerable to this type of attack!) Raid 1 drive arrays in servers and storage systems are also vulnerable to another form of attack. While the array is powered down, it is quite simple to remove the drive mirror and replace it with another. I have not heard of an instance of this occurring, but have tried it myself. Unless you are checking your logs regularly, it would be quite easy to miss this.

Workstations, laptops and PDAs – While it is true that workstations and particularly laptops are prone to theft, there is another, costlier, major concern: they often provide in-roads into your servers. For this reason, physical security of administrators' workstations and laptops should be a major concern. Even if they are not stolen outright, access to these systems can offer an intruder user ids, passwords and insight into your network. Most administrators, even the anal ones, tend to be creatures of habit and use variations of if not the same user id's and passwords for several purposes. Using the same methods outlined in the server section of this paper, an intruder can pretty much compromise your entire network. Ensure that you have disabled booting from floppy or cd-rom and then password protect the BIOS. You should also consider sealing a workstation with some form of tamper resistant tape. If you discover the tape has been damaged, you may also discover the BIOS password has been reset. At that point you have a genuine reason to be concerned.

PDA's are a relatively new security concern. Many administrators and security professionals use them to store ids, passwords, ip addresses and any number of items that could be used to compromise a system. Because of their size, they are very easily stolen. If you do store administrative information on your PDA, take the time to invest in a good encryption application. Even then, a good encryption program only offers you time but if you are abiding by standard system security policies concerning password changes, that should be all you need.

Backups – Your backup tapes are particularly vulnerable to theft due to their small size so extra care should be taken when securing them. If they contain particularly valuable or sensitive information, they should be part of a daily inventory scheme and protected at least as well as your servers. If you are storing tapes off-site for disaster recovery purposes (and you should be) you need to ensure the storage facility is as secure as your own. Even if your tapes are well secured, use a backup utility that incorporates a strong encryption scheme and make sure the encryption option is selected. Care should also be taken when disposing of backup tapes. Make sure *all* tapes are disposed of in such a way as to prevent recovery of information. Information can still be recovered off of old or defective tapes. I have even purchased supposedly "recycled" tapes that contained unencrypted, sensitive information (employee names, social security numbers, etc). Burning is an option, but there are several document grinders/shredders that can be used to destroy raw tape. Make sure any grinder/shredder you use is capable of destroying magnetic media or you may end up ruining one that isn't.

Theft control – “I know of a case in which a Novell NetWare 3.11 server was carried out the front door of a bank by two ‘repairmen.’ The support person discovered the server was missing only when he got a ‘server missing’ message during the evening backup.”[1] One thing about physical security is that it is pretty independent of operating systems. I could walk out of an insecure facility with a Solaris server just as easily as I could with a laptop. If you happen to work in a facility with a moderate level of security, chances are there is probably a pretty good theft prevention program in place. Take the time to review it and make your co-workers aware of it. If there is no loss prevention policy or procedure, implement one of your own. Even a simple sign-out procedure is better than nothing.

Documentation – We all know how important it is to properly document our systems and networks. In addition to helping with disaster recovery, good documentation can actually prevent inadvertent damage or disruptions to your networks and systems. Take the time to accurately describe the cabling endpoints. Note the location of important power breakers. Be as specific as you can when describing the infrastructure surrounding your data.

On the flip side, your accurate documentation is also a tempting target to anyone with plans to disrupt your systems or steal your data. It requires the same level of protection as your most sensitive data if not more.

Security Plan – This is where the rubber meets the road. Three things have to occur in order to consider a physical security plan a success:

1. There must be a single security point of contact for your systems. The person needs to have the authority to enforce the plan.
2. Your fellow employees need to be familiar with the physical security plan, policies and procedures and abide by them.
3. Your management needs to be willing to support and enforce them.

Unless you have acceptance and accountability from all three, a security plan of any sort is next to worthless.

A physical security plan needs to be a living document. Never assume you have covered all your bases. I have only barely covered a small number of physical threats and solutions. Adapt and improve on it as you discover new weaknesses and challenges. If you do not have a physical security policy or plan in place

[1] Moskowitz. http://www.networkcomputing.com/1202/1202colmoskowitz.html

already, take the time to document the “what” and “who”. Then take the time to discuss and implement the “how “ with your facility security manager if you are lucky enough to have one available. If not, take the time to create a physical security plan of your own and implement it.

Your security options are going to cost money and resources; some more than others. In most cases, you are not going to be given a blank check. You are going to have to get management buy-in and this is where being thorough is going to pay off. By explaining the weaknesses of the current system, giving them options and explaining the benefits and costs of each choice they are far more likely to understand and support your suggestions.

In the beginning, I described a recent event which prompted me to write this paper. In this particular case, a facility safety employee and fire marshal were allowed to enter the data center. The fire marshal was there to test the fire alarm systems. The fire sensors in this data center require two separate indications of a fire in order to trip a fire alarm. While testing the sensors, the fire marshal simulated both. At that point, the fire alarms sounded and ALL power was cut to the data center including UPS and backup generator. The fire system worked as advertised and had there been a fire in the data center, the firemen would not have had to worry about an electrocution threat. While restoring the power, the electrician was not aware of the safety interlock located in the data center UPS. The interlock was tied directly to the fire alarm to cut power in the event of a fire in order to prevent electrocution. Once the interlock was found, power was restored and the systems were quickly brought back on line. What could have prevented this? A simple access list. Only key personnel and security had the combination to this data center but as the data center was relatively new, and there was not yet a central point of contact for systems security, an access list had not yet been created. I have also mentioned being aware of critical power circuits and their breakers. In this instance the breakers were securely behind locked and guarded doors; however, it took several hours before the electrician became aware of the interlock and reset it. Basically, a preventable accident took down our million-dollar data center and affected several customers as effectively as a malicious attack.

Conclusion

To fully cover physical security is beyond the scope of this document but it is far too important a subject to ignore. By now you should be at least a little paranoid and a little paranoia can be a good thing when dealing with your data.

I have had a particular O’Reilly book now for several years, which pretty much sums everything up nicely. “In some ways, physical security is the easiest and the most rewarding type of security. It’s very visible and reassuring. It’s a tangible signal to employees and clients that you take security seriously"[2]. I don't think I agree fully with it being the easiest type of security but physical security certainly sends a clear signal when implemented properly.

[2] Deborah, p. 238.

References:

http://www.cert.org/octave/

http://csrc.nist.gov/fasp/

Moskowitz, Robert. “Let’s Get Physical” 2 January 2001
http://www.networkcomputing.com/1202/1202colmoskowitz.html

http://fas.org/irp/doddir/army/ar380-19/chap2.htm#SECT2-10

http://www.dooraccesscontrol.com/biometric_access.htm

http://www.voltec-industries.com/pdf_files/Adapters.pdf

http://www.winternals.com/

Russel, Deborah I and Gangemi Sr, G.T., Computer Security Basics, O’Reilly & Associates, Inc, 1991, 238