Global Information Assurance Certification Paper

Implementing Robust Physical Security

A Lord of the Rings

Bob Pagoria

July 13, 2004

GIAC Security Essentials Certification Version 1.4b

Table of Contents

Abstract
As the world of computer technology continues to grow, becomes increasingly competitive and vulnerable to malicious attacks, every business must more seriously consider IT (Information Technology) security as a high priority. IT security has become increasingly important over the past fifteen years due to the implementation of LANS (Local Area Networks), WANS (Wide Area Networks) and the Internet, all which provide a means of exploitation from unauthorized users. The information presented provides insight and direction on one of the most important rings of IT security, physical security. It will also provide information regarding the rings physical security itself contains and requires, ensuring the most complete, effective and robust physical security policies are implemented; all to help thwart the possibility of attack and loss of company resources.

Since the terror attacks of 9/11, it has become abundantly clear physical security is a critical issue (3) "Synergy in Security" (http://cyberdefensemag.com/feb2004/articles4.php) and can no longer be taken lightly. This holds true for all businesses, regardless of their size. New demands and more dollars are being invested more than ever to ensure proper measures are being taken in all areas of physical security. There are key factors which further impact the need for companies to invest in and implement a more robust physical security model. In this manuscript, we will examine what these factors are, how they may impact business and the level of importance each of them represent. Physical security is the first line of defense in the exploitation of computer systems, which can cost companies exorbanent amounts of money, resources and time. The objective of this manuscript is to encourage thorough and complete research by all companies, for implementing a more robust physical security model. Let's take a look.

Remember Physical Security
Whether it's a small business or a large business, Information Security must be a key area of concern and focus. Information Security can make or break any business from a financial or competitive perspective. When considering and researching Information Security, there are different rings of security to consider. One of the most important or first ring of security to consider is physical security. One of the least technical methods of information security exploitation is the breaching of the physical security ring. Exploiting the physical security of any company requires minimal, if any, technical knowledge on the part of the intruder. Many times physical security is compromised inadvertently by someone who had no malicious intentions whatsoever. For example, a company's custodial worker is vacuuming the floor of the company server room. As the custodian vacuums under the server table, he or she inadvertently snags the server power cord with the vacuum and pulls it out of the wall. Without the proper physical security safeguards or controls in place, this particular accident could cause the server to shut down. This may seem like a benign incident, but due to the hard shut down, could potentially cause sever malfunction when rebooted. This could result in

company down time and negatively impact production, all of which could ultimately cost the company money.

Just as there are rings of security in Information Technology, there are also rings within physical security. They are:

- Ring 1 - Areas on the perimeter of the business building
- Ring 2 - Immediate area around the business building/environmental
- Ring 3 - Internal location of the business building
- Ring 4 - Human factor

It is critical each of these four rings are thoroughly researched, addressed and implemented when incorporating an Information Security model in any business. Each one of these rings will be discussed and addressed in the upcoming sections of this manuscript.

Physically securing computer hardware should be any company's first step in securing their IT business. Without first implementing physical security, all other security measures may be meaningless. Thousands of dollars can be spent on implementing the most current IT security technologies on company severs, but if they are not physically secured, this may prove to be a costly lesson. Virtually anyone has access to those servers and can perform malicious or unintentional damage to them. An example of this would be a company spending thousands of dollars to secure their servers by installing firewalls, encryption and virus software. However, there was very little thought in the implementation of securing the physical access to those servers, which reside in an unrestricted area. Since there is no security for entering the server room, anyone could easily access the servers, which permits them the luxury of working to exploit the security controls installed on the servers and obtain critical information. This could also result in the physical theft of the servers. One of the most effective security steps this company could have taken was to first prevent an attack on the servers by implementing physical security controls for access to them.

Implementing a robust physical security model is critical for all businesses to help ensure computer integrity and availability. It is the first step in ensuring computer hardware protection against malicious and even inadvertent activities which can cost the company money, time and a competitive edge. Physical security and its four rings should not be forgotten.

Physical Security and Environmental Factors

Implementing a physical security model in must include the consideration of environmental factors and implementing environmental security controls. Environmental factors represent the third ring of physical security. When surveyed, more than seventy percent of risk managers believe environmental hazards pose the greatest security threat to a company's earnings (1) "Tech Talk: Prepared for Disaster" (http://www.securitymanagement.com/library/001465.html).

Some of these environmental hazards include; fire, floods, moisture, electricity and temperature; all of which can have a profound negative affect on IT computer components and equipment. The survey also showed companies are much more prepared for environmental interruptions than they were one year ago, due largely in part by the painful reminder of the 9/11 terror attacks.

A key issue in the consideration of environmental protection is the availability and continuity of computer systems. Computer systems require redundancy in power availability. If the electrical power to the computer systems' building goes down, a backup device needs to be ready to take over and keep those systems powered up. This can be accomplished with two types of devices, a UPS (Uninteruptable Power Supply) or a power generator. Power generators can be used for maintaining overall electricity in the company building for such things as lighting and general power, but can also be utilized for maintaining computer power in the untimely event of a power outage.

The UPS is used primarily for the supplying of electricity to the company computer boxes or servers. If a company server loses power, and there is no backup in place, the server will shut down resulting in loss of use and loss of productivity. However, with a UPS, if the electricity to the server is lost, the UPS will take over. The UPS battery source will provide the needed electricity. Although the supply of electricity is limited, it generally provides enough time to keep the server running until the electricity is restored. Some UPS units will sound an alarm to alert the IT administrator, to safely shut down the computer box and avoid a hard shut down. Another function of the UPS is to intercept power spikes and prevent a spike form reaching computer equipment. Power spikes can be dangerous to computer equipment and result in costly damage.

Fire hazards are another area of protection needing to be planned for by all companies. Risks from these hazards can be addressed by investing in smoke alarms, heat sensors, fire extinguishers and sprinkler systems. These devices may go a long way in preventing any substantial damage to computer systems and most of them are relatively inexpensive. It is also important to ensure staff members are trained in the use of these devices. Regular inspections of these devices should also be conducted to ensure optimal operation. These inspections should be completed at least twice per year by a certified professional or the fire department. Smoke alarms should be installed inside the computer room and directly outside the computer room. These fire alarms should consist of both manual and automatic operation. There may be times when a person detects a fire long before an automatic smoke alarm, therefore, the manual alarm can be engaged and further fire damage may be prevented.

Heat sensors should also be installed inside the computer room and directly outside the computer room to warn of any significant rise in temperature. These devices are easy to install and will emit an audible or visible alarm.

Every computer room should have at least one fire extinguisher. The fire extinguisher can be used once a fire breakout has been detected. There are two types of fire extinguishers to consider; the traditional, dry chemical extinguisher or the halon gas extinguisher. The dry chemical extinguisher may cause further damage from the chemical material it dispenses. The chemical material the extinguisher contains should depend on the type of fire; for instance wood fires, solvent fires, and electrical fires. The extinguisher should be labeled to specify the chemical material it contains by the following: (10) "Fire Protection" (http://www.fmca.com/motorhomingguide/safety/fireprotection.asp)

- Class A – wood, paper, cloth rubber and some plastic material
- Class B - liquids, gasses and grease
- Class C – electrical sources
- Class D – magnesium and sodium

The halon gas extinguisher dispenses a gas which deprives the fire of oxygen to extinguish the fire. This may result in less damage to your computer systems. However, the use of halon does present some environmental concerns, whereby it may be a factor in the depletion of the ozone layer. A 1997 agreement, called the Montreal Protocol, called for a cessation of halon due to its effects on the ozone layer (10) "Fire Protection" (http://www.fmca.com/motorhomingguide/safety/fireprotection.asp) Sprinkler systems known as wet-pipe and dry pipe can also be installed. The wet-pipe is a sprinkler system with all the piping filled with water under pressure. The dry-pipe is a sprinkler system with the piping filled with air pressure. When a sprinkler head opens, air is released and water flows into the pipes and to any open sprinkler head. The dry-pipe is utilized to prevent potential freezing of the pipes and causing further damage.

Water damage is another environmental hazard to consider when physically securing your computer systems. Water damage can occur from leaky or broken water pipes, flooding and even internal sprinkler systems. In order to help prevent or mitigate water damage, water detectors may be installed on the floor or under a raised floor near the computer equipment. Additionally, water-proof covers should be made readily available in the event of a water hazard incident.

Temperature regulation is also critical to preventing environmental losses. In order to prevent computer damage due to temperature fluctuations, it is important to store all computer equipment in a dedicated computer room. The computer room should be set to the appropriate temperature and humidity level to ensure optimal and continuing operation of the computer equipment. The computer room temperature should be set to sixty to seventy five degrees Fahrenheit. The humidity level should be at twenty to seventy percent and monitored regularly. (11) "NSC: Physical Security" (http://security.uchicago.edu/docs/physicalsec.shtml)

One of best preventative measures any company can implement is a Company Contingency Plan. The contingency plan should include all the scenarios just described here and the necessary steps to be taken to get the company back into a recovery and production mode. The plan should be completed by a committee of representatives from many areas such as Human Resources, Administrative Services and IT. Obviously, smaller companies or businesses may not require such a diverse committee, but nonetheless should implement a contingency plan to fit their needs. The contingency plans should include such items as:

- Server backup and recovery
- Data backup and recovery
- Network backup and recovery
- Employee backup

Obviously, this is not an all-inclusive list. These are examples of some of the key items needing to be addressed and planned for.

Physical Security and Human Factors

One key ingredient of any recipe for computer exploitation is the human factor. Whether it's intentional or unintentional, statistics show more than eighty percent of all computer exploits stem from internal or authorized users of the systems. (2) "Security Synergy" (http://infosecuritymag.techtarget.com/articles/november01/industry_synergy.shtml). This has forced companies to take a more hard lined approach to the word trust. Aside from this statistic, companies must also plan for the other 20% of exploits from occurring, which include an external or unauthorized user.

One of the easiest and most common ways to prevent unauthorized access to any company is to incorporate perimeter security. This can be accomplished by utilizing security personnel, surveillance cameras and fences. Any one of these methods can be very effective at preventing an unauthorized user from entering the premises. These same security methods can also be used for the immediate area around the building. One other method which will work well for both of these scenarios is employee training or awareness. Ensure employees are properly trained in the area of security awareness. This will help them to identify and report any suspicious acts on or around the premises. Utilizing all three of these methods will also work well for securing the internal location of the business building. Other methods for securing the internal location of the building include the use of more modern technologies such as, door locks requiring access code entry, motion detectors, magnetic card swipes, biological recognition (such as fingerprints, voice or retinal scans), or a combination of two or more of these technologies. Many of these also track the access activity of the individual or create an activity log. It is important to note, the biological or biometric security technologies take security a step further in ensuring authorized

access. This is due to the unique recognition of physical credentials all humans possess.

But, let's not forget, the overall level of security is only as strong as its weakest link. Installing more sophisticated methods of authorization may not be enough. We must also think about other ways unauthorized users can acquire access such as, windows, air ducts and social engineering. This may sound far fetched and more work than it is worth, but it is nonetheless something to be considered in the overall physical security model. These are possible entry ways into any company which may not require authorization, detection or prevention. Depending on the size, complexity and available funds for any business, not all of these methods are practical, but should at least be researched. This is not a one size fits all concept; businesses will have to implement what is appropriate for them and suits their needs.

Now, what about the eighty percent we talked about earlier? What about the physical protection of accesses from internal, authorized users? Many times, internal attacks are accidental. These attacks can be prevented by incorporating many of the environmental precautions we talked about previously such as, installing a UPS, ensuring fire extinguishers are available and functional, ensuring heat sensors, smoke alarms and sprinkling systems are installed and employees are educated. Accidents happen all the time and many times they are caused by human error. These devices will help greatly in mitigating that risk. Then there is the intentional attack by authorized users. This is the most difficult to prevent and happens more in larger companies. If an individual was trusted with certain access rights, the company is trusting they will not compromise the access they have been granted. But, sometimes it just doesn't work that way. The best thing a company can do to prevent this from happening is educate other employees so malicious attacks are identified and reported. Another preventative measure is to incorporate any of the logging or tracking mechanisms we discussed. This would include surveillance cameras, security personnel or biometric devices. Although neither of these methods may be able to prevent an internal malicious attack, they do make it possible to react to one which may help recover from it or prevent it in from reoccurring in the future.

Physical Security/Information Security Integration

Considering the whole concept of IT security, physical security must be included in the information security model. In other words, physical security must be integrated into any company's information security model. Thinking about security in these terms, is physical security really a separate issue or is it inherently just 'information security', period? The answer is, maybe; maybe not. It really depends on the current or future scope of a company's existing information security model. Many pre-9/11 companies implemented negligent physical security policies and have worked, or are working to make them more robust. Its not that they didn't want to spend the money to implement a more robust physical security model, but they really never felt the need. Many post-

9/11 companies follow the concept of physical security and information security being one in the same. But it is nevertheless true, enhanced physical security can improve information security. Some examples of this include:

- Use of biometric authentication for building and network access since identification badges can be easily compromised
- Always escort third party personnel into the building and never leave them alone
- Implement a security awareness program or social engineering course for all employees
- Implement a security ID card used for building and information access authorization
- Conduct thorough and complete background checks on all IT employees

All of these examples not only enhance the information security, but will enhance the overall security of any organization of any size.

The discussion of physical and information security integration, must include the OSE (Open Security Exchange). The OSE was formed in 2003, and is an independent, cross industry forum that addresses and promotes security integration in today's security infrastructure management (8) "Physical Security Bridge to IT Security PHYSBITS" (http://www.securitymanagement.com/library/Physbits_tech0703.pdf). The OSE works closely with existing standards bodies to create interoperability standards. One of the interoperability standards the OSE is currently working on is bridging the gap between physical security and information security or PHYSBITS (Physical Security Bridge to IT Security). One of the techniques or processes the OSE is focusing on is linking the physical security network to the IT network so when an employee badges out of the building at 3:00, but authenticates into the IT network internally at 8:00, a red flag is raised. In the past these events were not linked together and no red flag was raised. This integration solution will help companies and businesses reduce costs, while at the same time, reduce security risks. This can be accomplished by the following:

- Reduce the number of systems needed to monitor physical security and IT security
- Reduce the number of IT employees needed to monitor physical and IT security activities
- Mitigate the occurrences of unauthorized access to the IT network
- Centralize security events monitoring
- Flexibility in tracking events linked to physical security and IT security
- Reduce the number of credentials needed in the company's infrastructure

Statistics show, seventy percent of data theft is physical theft (5) “Time to Marry Network and Physical Security” (http://software.silicon.com/security/0,39024655,39120304,00.htm) from such devices as laptops, hard drives and other storage devices. It is also painfully true; adding more and more firewalls to any network will not prevent the theft of these physical devices. So it becomes increasingly obvious companies need to cross reference IT network activity and physical activity to prevent and detect malicious attacks within their infrastructure. Integrating the logical with the physical world will enable companies to take more control of their enterprise by digitally identifying an employee as they enter the building and digitally identifying the same employee’s activity on the company network. This will provide the company with a much clearer view and perspective of employee behavior. This will allow for a more efficient and effective way of preventing and detecting malicious behavior. So, in conclusion, IT security and Physical security are no longer security silos in the IT environment, they are and must be considered one in the same or as it is should be called, overall security.

Physical Security and Financial Factors

The underlying objective of implementing a more robust physical security model also goes a layer deeper than just protecting information. Physical security is also needed to prevent large financial losses. Considering a standard laptop goes for about a thousand dollars, it is obvious a negligent physical security model may cost a company thousands or even millions of dollars per year. The same holds true if that same laptop is destroyed by an environmental incident. Regardless of the size of any company, the financial losses due to physical security breaches and environmental losses may be unrecoverable.

According to the 2003 Protecting Value Study (survey of approximately 400 CFOs and risk managers) one of the greatest threats to any company’s earnings is environmental hazards (1) “Tech Talk: Prepared for Disaster” (http://www.securitymanagement.com/library/001465.html). This includes such hazards as fire and natural disasters. This also includes physical losses due to theft and employee practices. This same survey also discovered companies are much more prepared today for contingency planning than they were a year or two ago. Much of this turn around has to do with an increased awareness of physical security importance since the 9/11 terror attacks, and an upfront investment in a more robust physical security model. If we take into account all the scenarios we discussed involving physical security, they all have financial implications. For instance:

- Human factors – These costs include situations whereby employees may intentionally impact a company’s bottom-line by physical or information theft or malicious network attacks. This also includes unintentional impacts to the company’s IT network such as inadvertent sever shut downs. This will cost the company dollars due to employee down time, loss of production and potential computer repair costs. The

dollar amount will vary depending on company size, length of down time, computer damage and employee salaries.

- Physical and IT Security Integration – In an effort to implement a more robust, centralized security model, to mitigate overall financial losses, companies are investing in security integration. There is an upfront dollar cost in implementing integration, and an ongoing maintenance cost, but may save a company more dollars in the end by preventing or mitigating ongoing security fraud.
- Environmental Losses – This includes such disasters as fires, floods power outages and temperature changes. Environmental losses are virtually impossible to predict which means the financial impact is also impossible to predict. All any company can do to prevent loss in this area is to prepare as much as possible and implement a redundancy or contingency plan for their critical daily operations. Without this planning and depending on the cost of the losses, a company may not be able to withstand the financial losses.

One more important financial impact all companies, small or large, must consider is legal costs. This is also more crucial then ever before. Not only are companies more susceptible due to technology advances, competition and malicious attacks, they are also more susceptible to legal action against them. Depending on the allegations made against them and the size of the company, lawsuits can be very costly and even warrant company shut down. A robust and well planned out physical security model can greatly reduce the possibility of large legal fees. For example, with the use of biometric technology, biometric information must not be gathered without the knowledge and sign-off of company employees, vendors or third party associates. Additionally, the biometric information must not be used for purposes other than what the employee or visitor agreed upon originally. If it is, the company is prone to legal action being taken against them. Another example of potential legal action is the unauthorized releasing of personal information regarding another company employee. If systems are not properly secured from unauthorized access, confidential information may be obtained, resulting in legal action against the company for failure to protect personal and confidential information. These types of offenses may also cost the company large amounts of money due to fines imposed upon them.

The bottom-line is it is about the bottom-line. In order for companies to remain competitive and profitable, a more robust and effective physical security model must be created and implemented. Yes, there are dollars to invest, but the investment may prove to be worthwhile and less costly if the physical security model is not revisited and updated accordingly on a regular basis.

Final Thoughts

We have covered many different aspects of implementing a more robust physical security model for any company or IT shop. Physical security can no longer be

considered a low priority in any business wanting to obtain or remain competitive or profitable. All areas of physical security must be thoroughly researched and all rings of physical security must be implemented to some degree of complexity. Of course this will depend on the size of the company or IT shop. When a company is looking to define or redefine their security model, physical security should be automatically included. Yesterday, physical and logical security were considered as two separate entities but today, there spoken it he same breadth, as well they should be.

There are no cookie-cutter physical security models. Physical security models need to be created to fit the individual company or business needs. Each company or business needs to implement what they can afford and what makes sense for their environment. For instance, what may be feasible and practical for a company employing two hundred employees will most likely not be the same for a company of two thousand. But, the concept of 'robust physical security' is identical to both companies.

It is important to remember one important point about physical security, as long as there are people, there is a potential for security compromises and attacks. These may result from a malicious attack or an inadvertent mishap from inside or outside the company. Natural mishaps are also a factor which can not be eliminated. Both of these scenarios warrant some level of prevention and reactionary measures. Of course they can all me avoided or mitigated by ensuring the physical security model is robust and right for the company whether regardless of it's size.

References

(1) **Piazza, Peter "Tech Talk: Prepared for Disaster" URL: http://www.securitymanagement.com/library/001465.html (July 2003)**

(2) **Schwartau, Winn "Security Synergy" URL: http://infosecuritymag.techtarget.com/articles/november01/industry_synergy.shtml (November 2001)**

(3) **Graves, Jack "Synergy in Security" URL: http://cyberdefensemag.com/feb2004/articles4.php (February 2004)**

(4) **e-Newsletter Archive, Domino Wire System Admin Tips Newsletter "Don't Forget About Physical Security, Even in Small Shops" URL: http://www.e-promag.com/epnewsletters/index.cfm?fuseaction=ShowNewsletterIssue&ID=839 (May 13, 2004)**

(5) **Sturgeon, Will "Time to Marry Network and Physical Security" URL: http://software.silicon.com/security/0,39024655,39120304,00.htm (April 28, 2004)**

(6) Mimoso, Michael S. “Time to Narrow Gap Between Physical/IT Security” URL: http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci924496,00.html (September 11, 2003)
(7) University of California “Environmental and Physical Security Controls” URL: http://security.ucdavis.edu/physical_security.cfm (September 2, 2003)
(8) PHYSBITS “Physical Security Bridge to IT Security PHYSBITS” URL: http://www.securitymanagement.com/library/Physbits_tech0703.pdf (April 14, 2003)
(9) Fickes, Michael “Bridging the Gap” URL: http://securitysolutions.com/mag/security_bridging_gap_2/ (April 1, 2004)
(10) Busick, Stephen K. “Fire Protection” URL: http://www.fmca.com/motorhomingguide/safety/fireprotection.asp (October 1996)
(11) The University of Chicago “NSC: Physical Security” URL: http://security.uchicago.edu/docs/physicalsec.shtml (2000)