GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec



Computer Rooms – Meet the physical security measures

(GSEC – Assignment 1 version 1.0)

Felicitas Guil

April 2003

© SANS Institute 2003, Author retains full rights.

ABSTRACT

This paper will give several recommendations on how physical security, especially in the computer room, could be improved. Physical security is often neglected or not implemented appropriately. This document is thought to raise the awareness and to point out the importance of physical security. It will offer some suggestion on what should be thought of and addressed when looking into this sensitive area. The document is divided in the main areas of physical security controls, additional recommendations and computer room policy. The paper will end with a conclusion.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Table of contents

1. INTRODUCTION 3
2. OBJECTIVES 3
3. THREATS 3
4. PHYSICAL SECURITY CONTROLS 4
Administrative controls 4
Physical and technical controls 5
5. ADDITIONAL RECOMMENDATIONS 6
6. POLICY FOR COMPUTER ROOMS 7
7. CONCLUSION 10
8. REFERENCES 11

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

1. INTRODUCTION

Physical security is quite a static area with well defined threats and risks as well as controls to be implemented. It is fairly a straightforward process often with non-technical requirements on how to improve the overall security. For many people this security topic is not of much interested and some cases have shown that companies often do not have the proper physical security in place [1].

What is physical security? Physical security is the need to protect the company's information assets, IT services and resources as well as ensure the safety for the personnel. It provides the basics for IT security but is often overlooked or not implemented adequately [2]. The security impact could be ample if an unauthorized individual can get physical access to your computer because most of the logical security controls can be overcome fairly easy once the physical barrier has been overcome.

Like logical security the physical security is to be implemented to meet the three basic security objectives: confidentiality, availability and integrity. Depending on the information assets and kind of risks you are exposed to it may be necessary to setup or improve the physical security of your computer room. Performing a risk analysis will highlight the threats, vulnerabilities and costs you may have to face in case that the physical security is compromised, intentionally or unintentionally.

2. OBJECTIVES

The fundamental demands for physical security to a dedicated computer room are the same like other targets for physical security, e.g. for the building: it's to ensure the main objectives of IT security, namely confidentiality, availability and integrity. Additional to those basic objectives physical security includes safety and authorized access. Personnel safety is the prime aim of physical security. Its goal is to protect people from harm and disaster and should always take precedence compared to other controls. The latter should also be applied even if there is a trade-off with security. Those objectives should be taken into account when companies implement the physical security for computer rooms.

3. THREATS

The threats of physical security can be divided in three major areas: Emergencies, natural disasters and human intervention. Each of them could put C.I.A. or one of these at risk and represent a danger to the company. Emergencies include fire, smoke, water damage, toxins, temperature extremes, structural failures and loss of utility. Storm damage or earth movements are examples of natural disasters. The third threat area includes all manmade risks like vandalism, strikes or sabotage [3].

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

In areas where sensitive information is stored together, like servers in a computer room, any weak point could potentially lead to a bigger damage. It is important that proper controls are set in place.

4. PHYSICAL SECURITY CONTROLS

The physical controls are divided into two categories: Administrative controls and Physical/Technical controls. Details about the controls are well described in [3]. Computer rooms should meet following requirements:

Administrative controls

Facility construction

Computer rooms are ideally planned and designed within the blue print of a new building. This is the ideal case and gives you the possibility to implement the chosen physical controls. But there are companies which are located in older buildings. Those often do not have specific equipped computer rooms. In this case a modular IT Room may be a good solution [4]. Those rooms can be set up within an existing room at the size required. They can be fully mounted with access control, air conditioner, fire distinguisher, UPS, raised floors and suspended ceilings. Older buildings should be checked for aging damage which may impact or be a threat to the facility's structure.

Facility Security Management

Access to the computer room should be recorded and reviewed. It is important that you not only prevent unauthorized access but that you also detect unauthorized access or access attempts. Facility security management also includes the process of emergency. Emergency procedures need to be simulated on trained on a regular basis. Those evacuation simulations should be carefully planned, executed and supervised especially if you would have to leave your computer room doors and facility doors unlocked.

Environmental and life safety controls

The following controls should ensure that operation of the equipment in the computer room can be maintained and that personnel safety controls are in place.

Electrical Power

Computer rooms should receive steady electrical power to sustain the operation of the servers and electrical equipment within the room. It is a good practice to install two separate electrical power supplies connected into the room. This allows you to connect your servers with two different power supplies. A blackout of one supply will not lead to a general interruption of the services. Additionally, a UPS (uninterruptible power supply) system can bypass a short electrical blackout. Larger companies may have also a diesel backup to bypass longer blackouts. The latter two allow that the servers do not turn off uncontrolled and in unknown state but can continue to run for a certain amount of time. Such interruptions should provoke an alarm and inform your staff immediately. If the power supply can not be restored in a certain amount of time then the servers should be manually powered down in a controlled manner.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Fire detection and suppression
The computer room needs to be equipped with proper fire detection and suppression. There exist several products on the market and should be evaluated corresponding to the needs of the company. It is common to have additionally a fire distinguisher in each computer room. Those should be checked and reviewed regularly by specialized personnel.

Air Conditioning
Temperature and humidity should be maintained on pre-defined ranges. Within larger rooms it may be adequate to have ventilation systems to help circulating the fresh air. Temperature variations are critical especially when the temperature drops rapidly. This could produce condensation which may damage the hardware. Your maintenance staff should be clearly instructed about this.

Administrative personnel control

Prevent that your enemy is within your perimeters. It should be a norm of the department of human resource that they perform screening of new employees. Also, a process should be in place which ensures that access, accounts and authorizations are modified or removed when an employee changes job position or quits his job.

Physical and technical controls

Facility control requirements

The doors to the computer rooms should have a lock mechanism. This can be realized either with electronic, mechanical or prevalent door locks.

Facility Access Control devices

There are different methods to control access to the computer rooms. Depending on what kind of access control and facility control you chose you may have a better or worse overview of your access logs. On high security rooms it is recommended that employees use a personal identification, like badge and PIN. This will enable to allocate an access to a specific person and trace their actions. Remember, prevention is ideal but detection is a must.

Intrusion Detectors and Alarms

You may want to add some kind of intrusion detectors and alarms inside the computer room. Businesses often have motion detectors installed which are activated during the night when the last person left the room. An alarm can be connection to the monitoring crew or police station.

Computer Inventory Control

Servers and equipment within the computer room should be checked regularly on functionality and existence. The machines have to be checked that they work properly and that there is no damage to the devices. Also, it has to be controlled that all devices are still in place and no theft has occurred.

Media Storage Requirements

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Sensitive information on media should be stored in a secure place protected from unintentional events like fire or water and from intentional events like theft or vandalism. It is advisable to keep the backup separate from the server. This will prevent that in an event like fire not both server and backup will be damaged.

A general checklist for physical security can help you to determine the contemporary security level of the company. A good checklist can be found at [5]. Following links provides some best practices and recommendations which can be implemented [6] [7].

5. ADDITIONAL RECOMMENDATIONS

Computer room policy
Setup your own computer room policy (see chapter 6).

Classify information assets
It is important that you know which kind of information and data are on the servers. It is appropriate to classify the information assets corresponding to the security objectives of C.I.A. This classification will usually set also the requirement for the objects involved with the information. Objects can be applications, network, servers or computer rooms. A classification of your data helps you to determine the right requirements for the computer room.

Layers of security zones
Create defence in depth by dividing your physical structure into different access controlled security zones. The most sensitive zone, like a computer room, should be logically placed in the centre. This will set multiple obstacles until somebody could actually gain access to the room. The goal is to have fewer people with authorized access to every zone layer you are entering.

Room classification policy
If you have multiple computer room categories with different security requirements it may be helpful to have a separate document stating the controls for each room category. This will provide you with a standard so that every room of the same class has the equivalent security standard. It also will help when you have to prepare for a new computer room.

Monitor temperature through servers
If the company has a big computer room and only few temperature sensors are lined up then it could be useful to have a supplementary temperature information measured by the servers themselves. Newer servers often have a sensor installed and can record this information through a software agent. Such information could be forwarded to the company's monitoring team. This method will allow getting measured data from various areas in the computer room. It also may help to detect fluctuations earlier than with the general room sensors.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Convey regular security checks
The checks should make sure that the policy and process are implemented properly. Not conformities should be reported and measurements should be taken. A review through an external expert may gain inside into weak points which may not be obvious and unknown. Also, external reviews provide a neutral view and may help find solutions to minimize the threats.

Plan ahead
Just like any business unit the future requirements on the computer rooms should be planned ahead. It is important to know how much additional space will be required and how much capacity is anticipated from electrical power and air conditioner. Only with proper planning can be made sure that the rooms will satisfy the company's future requirements.

Security awareness
Sensitize your employees on security issues. Make sure that they understand the need for physical and logical security and how they can actively contribute to the company's security. Attentive personnel who challenge unknown people in computer rooms or other areas of the building may hinder a potential attack.

Backup policy
This policy may state what kind of media is used, how often backup is done, what data is backup and where the backup media stored. Often there is a backup in house and one at another site. Backup media should be store in a locked and safe place to prevent unauthorized access and unintentional damage. The process of disposal of old backups and how data has to be made unreadable should be included.

6. POLICY FOR COMPUTER ROOMS

Many organizations have policies like security policy, network policy or internet use policy but some miss on a policy for computer rooms. The goal of a policy is to define the company's required and proper security standard for the defined area. The policy should not be static but instead should live and be reviewed and revised regularly. There are various types of policies but all should address purpose, scope and responsibility [8].

The following topics should be included in the policy:
Purpose
First, the computer room policy should clearly state the purpose and aim of the policy. This chapter specifies why the policy has been setup and what kind of advantages it will ultimately deliver to the company. This will help the employees to understand the goals and benefits of the procedure.

Scope
Further, the scope is to be defined. State for which areas or rooms the policy has to be applied. This helps to set boundaries and makes it clear where the rules will have to be implemented.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Responsibilities
Make sure that you have discriminating organizational roles. Every role which is somehow involved in the policy should be written out in the document. Describe in detail the roles, position within the organization, duties and responsibilities. Employees need to be informed about the policy and processes involved. Training will help to make the employees aware of the criticality of computer rooms and gives to opportunity for them to ask questions. It is a good idea to involve those employees in the creating process of the document who will actually have to follow the policy. It will probably initially take longer to get all the requirements and inputs together but the processes and rules are afterwards usually implemented better. Ultimately an effective policy is depended on how well the people life upon the rules the company sets up. To be able to enforce the policy this document should also be approved and signed by higher management.

Following topics are recommended to be included in the policy:
Basic rules
The basic policy rules could demand that servers with sensitive information are to be placed in a locked and dedicated computer room with controlled access [9]. Furthermore there should be some rules defined for network components like routers and switches because they also can be used to compromise the company's assets. Those components should also be in locked areas with limited and controlled access.

Classification of the computer rooms
If the company has different computer rooms you may consider to classify the company's computer rooms into different security categories [10]. Often the information assets have different security requirements. Since implementations of security controls frequently have some financial impact it is recommended to pool together similar assets with the same security specifications. This allows a company to define specific and distinctive security controls appropriate to the data's needs.

Even the lowest rated computer room should fulfil some basic controls. Higher rated rooms should provide higher security. Requirements which could vary for the different room categories may include: interior, like constructional and technical requirements, doors, access control, windows, air conditioning, fire protection and Backup Power.

Computer labelling
Every computer and equipment inside the room should have an inventory number and should be labelled. Many servers look alike and a clear labelling could prevent human mistakes. Instead of unplugging or power off one machine a worker may take the machine next to it. It is advisable to have a standard label definition in the company. Label information may include information like IP address, server name, application name, team responsible for the server and phone number.

Standard racks

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Bigger companies with large numbers of computers may have the need for standard racks. Standard racks have the major advantage that they can accommodate multiple servers within one rack. The racks have standard measurements and most servers or network components will fit inside. In addition to better space utilization those racks have the advantage that they set a standard in the room. Cabinet doors can be closed and if necessary also locked. Furthermore they offer a better wiring method. The network cables can be properly laid in specific flutes at the back of the closet. This prevents that cables are hanging loose and unsecured in the room.

Room Access

Generally the principle of least privileges necessary should be applied. The policy should define how access to the computer room is regulated. This could involve the processes on how authorized employees like system administrators or network administrators can obtain access to the rooms. A separate process should be prepared which addresses special access like hardware deliverers or craftsmen. Guests should always be accompanied and not left alone in the rooms.

General Instructions

The implementation of physical security should avoid that unintentional events can occur. Therefore it is important that the people working inside the rooms follow specific instructions set for the sensitive area. A list of behavioural rules can be set up including what is strictly prohibited and what should be done. This list may conclude with information about emergency rules.

The following is usually considered forbidden:

- No food.
- No drinks.
- No smoking.
- Not allowing unauthorized or unknown persons access to the room.
- Not leaving packing material and not used material inside the room.
- Not execute work which emits dust without pre-informing the responsible person of the computer room.

Although some of those points may sound obviously for the system administrators or security officer for other people those rules need to be written out. It is not unusual that workers like electricians or carpenters have no specific knowledge about computers and are unaware of what kind of damage they could produce.

Following is a suggestion of what should or should not be done:

- All persons inside the room have to wear a personal badge.
- Labours which produce dust and have to be done inside the computer room need to be supervised. Special vacuum cleaners with specific dust filters have to be used.
- Combustible material has to be removed.
- Electrical tools are to be plugged into separate electrical sockets. Designated server electrical socket are not to be used.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Furthermore, some emergency information like the following should be added to the instruction list.

- Emergency phone number.
- Emergency exit.

Specific Instructions

This list could state specific instructions for the different roles defined in the computer room policy. They can provide some guidance and standard.

System administrators should be instructed to follow rules like [11]:

- Logout or activate the screen lock and turn off the monitor when leaving the computer room.
- No passwords should be noted down.
- Servers should be configured that they are not bootable from floppies or CD-ROMs.
- Before discarding old servers and other hardware the data has to be destroyed and made unreadable and irreproducible.
- System and network manuals should be stored in a locked cabinet.

Cleaning

This part of the document could state who is cleaning what and how often it is done and what kind of equipment should be used. Raised floors are favourably cleaned on a regular basis by specialized cleaners. Those workers are equipped with special cleanser appliances and are usually trained well. Normal cleaning can be done by the company's cleaning team and should be recurring scheduled. Computer rooms are prone to have a lot of loose cables. The cleaning personnel should be instructed what they are allowed to do and where they should pay attention to.

7. CONCLUSION

The overall security for computer rooms is dependent upon the physical security of the entire organization. Unfortunately, there are companies which don't implement physical security appropriately. In such cases an unauthorized physical access to a workstation can be performed easily [12] and could lead to serious consequences like lost of confidentiality or availability. Additionally, small enterprises usually don't have a separate computer room but should nevertheless take some proactive steps to ensure the C.I.A. of their assets. Examples may be to secure laptops with special lockers or store backup media in a locked cabinet to prevent theft. Bigger organizations, like hospitals or universities, often add an additional layer of protection by having a dedicated computer room for their servers and network components. A computer policy may give the advantage by standardizing important processes and improving the company's general physical security.

Remember, physical security is the key element to all other IT security measures. Your security is only as good as the weakest link in your chain. Unauthorized physical access to any server could have profound security consequences. Don't let intruders break your basis.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

8. REFERENCES

[1] Kabay, M. E. “Lax physical security.” NetworkWorldFusion. URL: http://www.nwfusion.com/newsletters/sec/2002/01311303.html (Apr. 17, 2002)

[2] No author. 1.1 SANS Security Essentials I: Networking Concepts. SANS Institute. (2002)

[3] Krutz, Roland L. and Vines Russel Dean. The CISSP Perp Guide. New York: Wiley, 2001.

[4] No Author. “Static IT Rooms.” Remtech, Total Solutions for your computing environment. URL: http://www.remtech.uk.com/_it_rooms/static.html (1999)

[5] Heare, Sean. “Data Center Physical Security Checklist.” SANS Info Sec Reading Room. URL: http://www.sans.org/rr/aware/data_center.php (Dec. 1, 2001)

[6] No author. “Best Practice Guidance in Physical and Environmental Security.” National Compunting Center, NCC, England. URL: http://www.ncc.co.uk/ncc/myitadviser/archive/issue5/business_processes.cfm (May 5, 2001)

[7] Lewis, Dick. “Computer Room Fortress.” Windows & .Net Magazine. URL: http://www.winnetmag.com/articles/index.cfm?articleid=22250 (Oct. 2001)

[8] Maiwald, Eric. Network Security: A Beginner’s Guide. California: McGraw-Hill, 2001

[9] No author. “5-Minute Security Advisor - Basic Physical Security.” Microsoft Corporation. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/security/5min/5min-203.asp (2003)

[10] No author. “Handbook 14 Physical Security Version 1.0.” Australian Communications-Electronic Security Instruction 33 (ACSI 33). Defense Signals Directorate, Australia. URL: http://www.dsd.gov.au/infosec/acsi33/HB14p.pdf (Dec. 20, 2000)

[11] Lehr, Chris. “More Physical Security Measures.” Windows & .Net Magazine. URL: http://www.winnetmag.com/Articles/Index.cfm?ArticleID=22258 (Oct. 2001)

[12] Cole, Eric. Hackers Beware. Indianapolis: New Riders, 2001.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.