Global Information Assurance Certification Paper

"The Oversight of Physical Security and Contingency Planning"

Andy S. Krupa
Version 1.2d
Security Essentials (GSEC)

"The Oversight of Physical Security and Contingency Planning"

In today's ever-changing world of information assurance and network security, it can become extremely difficult to keep up on the latest vulnerabilities, viruses, patches, trends, technology, hacker behaviors and activity. It's easy for the information systems security professional to get caught up in attending the logical aspects of security: reviewing log files, making configuration changes, troubleshooting, and other technical duties the job may require.

On a particularly busy day, a network technician was swamped with tasks. During the course of an hour, he became caught up in his work, telnet ting to one machine, logging into another and so forth. During this time, an unauthorized visitor had entered the workspace unescorted. While the technician typed away, the visitor managed to look over his shoulder and capture a user name and password to a critical server with sensitive information on it, without the technician's knowledge.

Although this is a hypothetical situation, it could easily happen and it proves a valid point: All too often physical security is overlooked, taken for granted, and in some extreme cases, ignored. If a company invests large sums of money to deploy logical security (i.e. firewalls, intrusion detection systems, virtual private networks, etc.) what is the benefit of these systems if there is no access control and physical security can be compromised at the facility itself? If an unauthorized individual can enter into an organization, slip any kind of media that's deemed sensitive into his or her pocket, or overlook an employee as a password is typed in, the security of the network has been compromised because physical security was overlooked.

Closely related to physical security is the issue of contingency planning or disaster planning. If a flood, fire, or hurricane occurred at an organization's site, one would hope employees at this facility know what to do. More importantly, if there was unrecoverable damage to systems, there should be a contingency plan that gives accurate instruction on how to recover from disaster in a specific amount of time. Statistics provided by Price Waterhouse Coopers reveal that 90 percent of all companies that experience a computer "disaster" with no pre-existing survival plan go out of business within 18 months (Lyons, http://www.contingencyplanning.com/article_index.cfm?/articl

e=290.). It has been proven that a lack of contingency planning in the case of a disaster (whether it be flood, fire, or theft) will lead to a loss of functionality, time, resources and perhaps most importantly, a loss of service that the data systems provide. In the following pages I will address the importance of physical security and contingency planning. I will also discuss basic concepts that strengthen physical security for data networks, such as access control and basic physical security principles.

If a business or corporation has any data that they would consider sensitive, it's imperative that they employ access control policies to prevent theft or damage to the organization's data systems. Some organizations have one facility or office space that houses all data systems, sensitive or not. Others have multiple facilities. The first step would be to decide who should have access to which system or workspace and post an access roster that states this clearly at each location. One way to provide access control is the implementation of a badge system. Each person wears a badge with his or her picture, name, and organization. The badge system can be set to only allow certain individuals into certain areas, and deny access to anyone without a badge. This is only one example, as there are many other ways to provide access control: numeric combination locks, biometric security systems, etc. It's important to note that all methods are flawed in some way (an unauthorized person could steal an employee's badge) so it may be a good idea to implement two security features (a badge system that also requires a personal identification number that only the employee knows).

From time to time, every organization will have the need for visitors to enter their facility or workspace. Whether it is a maintenance employee repairing the air-conditioning, or a software vendor marketing a new product to management. A visitor in an organization's facility can be a security risk, but the risk is greatly increased if the visitor is not authorized to be there, or left unattended to do as he or she chooses. A simple way to remedy this problem would be to provide an accurate log at the entrance an office space, with someone there to keep track of visitors entering and leaving the building or room. As much information about the visitor as possible should be provided: full name, organization, phone number, social security number, reason for visit, and so forth. Also, the visitor should always be asked for identification and the organization he or she is visiting should be informed ahead

of time of their arrival. These steps will minimize the risk and increase the organization's security posture.

It is also important to note that physical security is not only the job of the information systems security manager, it should be the job of all employees who work for the organization. Annual or semi-annual security training for end users and administrators is a must. In order to maintain a strong security posture, members of an organization should know what to look for concerning security risks. Knowing how to report problems or incidents is also critical in maintaining that posture. Think of data systems as rows of slot machines lining the floor of a casino. Within the casino, there are guards, cameras, and alarms, not to mention the local security on the slot machines themselves. If someone wanted to learn how to break into a slot machine, they could buy one from the manufacturer, take it home, learn the ins and outs of the system, and learn how to break into it. How successful would the person be if he tried this inside the casino, with all of its security measures? The person would probably not get very far. But what if no one was watching? No security guards, and no cameras. The person breaking in would have a much easier time. What if the person could just take the slot machine home with him, no questions asked? Of course this would never happen, casinos are some of the most highly secured places in the world. Imagine for a moment that any group of servers in any organization are actually slot machines. What types of access control should be implemented to protect them? (Schneier, p 216-218) A good access control policy for an organization that maintains data systems plays an important part in protecting the data.

I have touched briefly on user/employee security awareness. It is another aspect that is often overlooked in many organizations. The majority of security violations and loss of data still originates from inside the organization. Therefore it is critical to monitor your organization internally and embed strong security practices into the members of your organization, especially the administrators of the data systems!

Much like the security practices of the casino, the careful placement of video cameras inside workspaces will assist security personnel in auditing events that take place day to day. It may make personnel of any establishment uncomfortable to know that they are being watched, however if there is a break in or a case of theft, the tapes provided by the cameras can be an invaluable tool. Granted,

this measure will not stop security violations directly. It will however help an information security team to enforce site security more effectively.

Another element that is important to a strong security posture is the security practices of the individuals that administer, maintain, and use the data systems at your organization. It is imperative that personnel are aware of what to do in the event of a security violation. They should also know what their personal responsibilities are relating to security practice. A good example of a poor security practice would be writing down a password and taping it to a monitor or keyboard. If a site security policy exists, this would likely be a clear violation. Another example would be leaving sensitive media unattended. If an administrator steps out for lunch and leaves a set of magnetic tapes containing his server's backups in an unsecured area, it's possible they could be stolen, lost, or damaged. Should the administrator be held accountable if the tapes come up missing, if he didn't know it was a violation of policy? The member of the organization *must* be held accountable for security violations. An excuse such as "I didn't know" or "no one told me" would not be acceptable unless there is no user awareness or user training. If the users are not aware of a policy, the policy itself will be ineffective. A good practice is to ensure you have a signed statement from each end user and administrator. It should state that they have read and understand the site security policy and their responsibility to ensure security regulations are followed. In addition it should be made clear that the user will be held accountable if they are involved in a security violation.

In 1992 the city of Chicago conducted maintenance along the Chicago River. Unfortunately, the work caused a rupture in the underground tunnel system and flooding ensued. When it was over, it had caused one billion dollars in damage, destroyed or disrupted numerous data and voice networks. As a result, 150 businesses were forced out of business.

Disaster can strike anywhere and at any time. The story above proves this. In the case of the Chicago flooding, contingency planning may have been able to save a large amount of the 150 businesses and their data networks.

A contingency plan should cover all possible scenarios that would result in a loss of data and property. Examples of this would be theft, fire, flood, or any other natural disaster possible in a geographic region. A first step would be to take a close look at disasters that have

occurred in the region, or could possibly occur. Insurance policies that cover all possible scenarios are a must!

Another important step is to compile a detailed list of all equipment including type, price, specifications, serial numbers, etc. Since incidents can occur at almost any time, the list should be updated on a regular basis. Within the contingency plan, it may be wise to specify a "response team". This would be a group of individuals that can respond in a short amount of time to a disaster or incident, as the contingency plan addresses. This step may save valuable time, and may determine minor damage from complete loss in the event of an emergency.

In the event of a disaster or loss of property, another policy to implement would be mirroring. If a company has two sites, one in Detroit and the other in Chicago, it would make sense for each site to have it's data systems mirrored from it's sister site, via WAN communication. This way, if the company's site in Detroit were victim to theft, all of its data would be copied in Chicago, and would make a restore much easier.

Ensuring monthly or quarterly tests on security alarms, emergency power systems, and fire protection can increase an organization's level of readiness. It is also a good policy to submit regular "readiness reports" to upper management and keep signed copies of these reports. The purpose being would be to show the organization did everything it could to prevent loss of property and data. Small details such as these can improve confidence within the organization, and within the customer if the organization is consumer-based. In addition, keeping copies of crucial documents (inventory lists, actual contingency plans, insurance policies and information) is a good practice, in the event a disaster should occur on site, and the original documents are lost.

In summary concerning contingency planning, Dr. Charles West of Contingency Planning and Management Online states the following: "In today's global business environment, being prepared to effectively manage the contingency of critical incidents is important to not only protecting your employees, but to protecting the bottom line as well." (West,URL:http://www.contingencyplanning.com/article_index.cfm?article=391.) This statement effectively sums up the importance of contingency planning in relation to physical security of data systems; the "bottom line" being the data systems that are being protected and the service they provide.

Throughout this paper I have addressed the importance

of physical security in relation to the protection of data systems and sensitive information. I have addressed the topics of access control, basic physical security practices, and the importance of contingency planning. In the fast paced world of information security, the information systems security professional must not overlook any risk or scenario, whether it is logical or physical. Only by implementing strong logical *and* physical security policies can data systems truly be secure.

References:

1. Schneier, Bruce. Secrets & Lies. John Wiley & Sons, Inc. 2000. 214-218.

2. Toigo, Jon William and Margaret Romano. Disaster Recovery Planning: Strategies for Protecting Critical Information Assets. Prentice Hall. 1999.

3. "Data Loss." 2000. URL: http://www.mammothtape.com/basics/dataloss.shtml.

4. West, Charles. "The Human Side of Disasters." August 2001. URL: http://www.contingencyplanning.com/article_index.cfm?article=391.

5. Berman, Alan. "Contingency Planning Assures Corporate Survival." 7 November 1997. URL: http://cincinnati.bcentral.com/cincinnati/stories/1997/11/10/editorial3.html.

6. Lyons, Jerry. "Let's Get Physical: Designing Secure IT Facilities." July 2000. URL: http://www.contingencyplanning.com/article_index.cfm?

/article=290.