Physical Security in the Information World

Robert Wall

East Carolina University

April 2014

In May 2013, the name Edward Snowden became known throughout the world. He made public highly classified documents that he had stolen from the U.S. National Security Agency. However, Snowden did not hack into a NSA mainframe to do this, nor did he intercept transmissions being sent across the Internet. Snowden had simply walked in and copied the information while doing his job, working as a system administrator on contract to the NSA. The NSA can probably be considered one of the most security-intensive organizations on the planet, but the theft occurred regardless. Laxity and a breakdown in physical security policy are to blame.

Physical security is a very important part of information security. It does not matter what kind of anti-virus software, intrusion detection software or firewall is installed on a machine if an individual can just walk up to it and take it. The concept of physical security has been around for thousands of years, and has been honed over time to account for numerous contingencies and to incorporate the growth of technology. However, in today's environment and in regards to information, there are a few concepts that should be considered when thinking of physical security: access control, the human element, and management. The combination of these three concepts can effectively mitigate the threat of information loss due to physical influences, both inside and out. Implementation of security will require careful planning and compromises in order to provide adequate protection without causing undue burden. Understanding the effective cost to an individual's or organization's resources and the value of the information to be protected will dictate how in-depth each of these concepts should be implemented.

Physical Access Controls

In regards to access control, there are many factors to consider. How much access restriction is appropriate to the value of the information, what options are available to meet these restrictions, and how it will impact the individual or organization are all important. A home computer does not require an armed security guard to watch over it, and a large government server room would not be served well by a simple lock on the door and nothing else.

For large organizations, using security guards can be an effective way to properly monitor and restrict access to sensitive areas. A security guard is not a static protection, like a door or a wall, and is capable of recognizing, assessing, and handling different kinds of situations. Some advice from the book The Complete Security Guide for Executives by Neil Livingston (1989) recommends that security guards should be serious about their job, be tactful and polite, and be sufficiently trained. A properly trained guard is able to address concerns of individuals they encounter, be proactive in the face of a threat, remain calm in crisis situations, and is able to handle routine and mundane tasks with professionalism.

One should consider the costs (like salary, training, and benefits) security guards add to an organization. A poorly paid guard has less incentive to be effective than a well-paid one. According to website Salary.com (2014), the median annual salary for a guard is $27,916 plus benefits. The cost of training said guards also needs consideration. One additional non-monetary cost is the impact to the organization's efficiency. Security guards, by necessity, will delay other individuals needing access to

guarded areas, slightly lowering productivity and possibly creating an environment of tension and frustration. By contrast, for smaller organizations and individuals, the costs associated with security guards preclude effective use.

An effective access control method for individuals and organizations of all sizes are locks. A locked door provides security by readily denying access for anyone who does not have the key, and is fairly cheap compared to hired security personnel. In addition, hardware can be secured through locking mechanisms that deter physical theft of the devices. However, not all locks are created equal and new technology provides better protection than a simple lock and key.

One of the new forms of locking mechanism incorporates biometric recognition. Biometric recognition in security applications analyzes human characteristics for identity verification (Faundez-Zanuy, 2006, p. 15). Characteristics that can be used for recognition include fingerprints, the human eye, or even a spoken phrase. Some advantages to biometrics is that they cannot be lost or shared, and are unique to each individual (Faundez-Zanuy, 2006, p. 15). Areas or devices secured with biometric recognition can only be accessed by individuals who have been cleared and set up with the appropriate biometric profile. A criminal cannot steal a passcode or smartcard to gain access to a biometric-secured area. Additionally, as technology progresses, sophisticated biometric devices are becoming much cheaper. A quick perusal of Google indicates fingerprint sensor prices close to $100, and even retina-recognition devices sale for about $3000, which is considerably cheaper than a security guard, while providing nearly the same amount of access restriction.

However, there are some disadvantages. As stated by Tang, Bringer, Chabanne, and Pointcheval,

> "Biometrics are usually regarded to be sensitive because they uniquely identify the individual. The sensitivity of biometrics lies in the fact that disclosure of biometrics in a certain application leads to the disclosure of the true identity of the involved users of the application. In addition, if the same type of biometrics of a user is used in two applications, then there is an undeniable link for the user's activities in both applications."

This profiling can make an individual uncomfortable with the use of biometrics and cause tension in the workplace. Also, biometric recognition is not completely fail-proof. A corrupted biometric profile will prevent access even to an approved individual. If an individual's biometric characteristic changes, such as through a scar on a fingerprint, than the profile becomes useless and has to be updated before access can be granted. While biometric locks are a great investment, these drawbacks must be considered.

The Human Element

Another aspect of physical security revolves around the human element, particularly as it relates to organizations of any size. An individual's personality and habits need to be considered before they are given access to important information. They need to be trained how to properly handle hardware to avoid physical loss of information. They must also be continually scrutinized for changes in their behaviors that may indicate a problem

To begin, organizations that deal in highly-sensitive or highly-valuable information should consider the advantages and disadvantages of background checks. As explained at website Privacy Rights Clearinghouse (2014), background checks

provide information on an individual's history and may include credit reports, spending habits, known acquaintances, education, and criminal records. This information can then be used to create a profile of a potential or current employee's habits, behaviors, and abilities. This can help determine the individual's trustworthiness.

However, there are some disadvantages to background checks. Some individuals feel uncomfortable with divulging personal information to such depth. Information found in a check may be incorrect or unfairly prejudicial, which in turn leads to false assumptions by the organization. Another problem is the trustworthiness of the background check itself. According to an article by reporter Michael Isikoff (2014), USIS, the agency that performed the background check on Edward Snowden in 2011, is being sued by the U.S. government for conducting 665,000 fake background checks between 2008 and 2012. If this turns out to be true, then the veracity of any of the checks performed becomes suspect. Also, the investigation that needs to be completed for a background check can have a significant monetary cost, depending on the depth of reliable information requested.

While personnel may be deemed trustworthy enough to be granted access to sensitive data, it does not mean that they will handle that data properly. Many news reports over the years have detailed how devices containing sensitive information have been lost or stolen. In the article "SECURITY GETS PHYSICAL" (2007), security consultant Cheng Tang is quoted,

> "Rather than hack a well-defended corporate network, smart criminals in search of sensitive information have discovered it's often more effective to focus on gullible employees and loosely guarded offices."

Individuals have to be trained to recognize the importance of the data they access, how to properly store data in a physical medium, and how to protect that medium from threats. This training, which may be costly, should be emphasized in policy and procedures, and should be periodically reviewed with employees in order to maintain high standards compliance. Failure to follow these procedures will most likely result in the loss of the data, which negatively impacts anything the data is related to in addition to damaging the reputation of the organization.

One last danger that the human element brings to an organization is the insider threat. An employee with a reason to steal information and that has the access to do so will. Employee behavior should be monitored in order to identify threats before they become a news story. Some of the personal behaviors to look for, as described in the book Crime Prevention through Physical Security by Walter Strobol (1978), include:

1. Dissatisfaction and complaints about too much work and too little pay.
2. Abnormally fearful of individuals in authority over them.
3. Lying or changing explanations when confronted with errors or discrepancies.
4. Displaying wealth out of proportion to current earnings.
5. Excessive or habitual borrowing.

These are just some of the warning signs that may be present, but all show an increase in the likelihood of an employee planning to or having committed theft.

Responsibility of Management

The last concept to be aware of is the responsibility that management has to coordinate the implementation, acceptance, and adherence to physical security policies and procedures. Managers must determine the value of information to be protected and the measures that must be taken to insure its protection. They must consider the costs

associated with those physical security measures, both monetary and time. Even individuals considering protections for their home must understand the ratio of value of information to cost of protection.

Management is responsible for dictating policy and procedures in regards to physical security. As outlined in the Security Managers Desk Reference (Post and Schachtsiek, 1986, p. 129), policies and procedures should be tailored to the particular organization and work environment. They should be written in such a way as to ensure that they deal adequately with situations that are most likely to occur. They should be reviewed periodically to make sure they are up-to-date and have been properly implemented. This process should begin, and periodically repeated, with a security audit or survey to determine where deficiencies existence in the current physical security structure. Lax access controls, improperly trained employees, or violations of current procedures need to be addressed. Employees need to be informed and trained when policies and procedures are implemented.

Managers are also responsible for properly budgeting for the expense of implementation and maintenance of a physical security plan. Purchasing and installing hardware, screening and hiring individuals, and training all will impact the budget of the organization. There is no catch-all method for determining how much to spend or what corners to cut. However, managers should be aware that the value of the information relates directly to the impact of that information being lost or stolen. Better security should be implemented for information that has greater possible impact.

One of the more important factors that managers are responsible for dealing with is the impact that security controls will have on the organization. Employees at all levels must be made aware of the importance that security controls provide to the safety of the information in their care. Inconvenience, irritation, and delay that occurs from being searched at a security checkpoint or denial of access by a faulty biometric scanner needs to be understood and addressed by management. Failure to properly consider the impact on the organization could lead to employees using improper methods to access information or employee anger, creating an insider threat. Management must be vigilant and ready to address the concerns of the organization when they occur.

In conclusion, these are just a few concepts that must be addressed and understood in order to effectively implement physical security. While not an exhaustive list, these three concepts form a core of competence that can be built upon to suit the needs of any size organization, or even a home office. The individual should understand that any physical security plan starts with a means to control access, understand the effect of the human element in any plan, and comprehend the responsibilities and cost that come with the implementation and continued use of the plan.

References

**Faundez-Zanuy, M., "Biometric security technology," *Aerospace and Electronic Systems Magazine, IEEE* , vol.21, no.6, pp.15,26, June 2006 doi: 10.1109/MAES.2006.1662038
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1662038&isnumber=34781

Isikoff, Michael (January 23, 2014). "DOJ accuses firm that vetted Snowden of faking 665,000 background checks". Retrieved from http://investigations.nbcnews.com/_news/2014/01/23/22401812-doj-accuses-firm-that-vetted-snowden-of-faking-665000-background-checks

Livingstone, N. C. (1989). *The complete security guide for executives*. Lexington, Mass: Lexington Books.

Post, R. S., & Schachtsiek, D. A. (1986). *Security manager's desk reference*. Boston: Butterworths.

Privacy Rights Clearinghouse (2014). “Fact Sheet 16: Employment Background Checks: A Jobseeker’s Guide.” Retrieved from https://www.privacyrights.org/employment-background-checks-jobseekers-guide

Roberts, P. F. (2007). SECURITY GETS PHYSICAL. *InfoWorld*, 29(5), 23-24,26,28,30. Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/194384296?accountid=10639

Salary.com (n.d.). *Security Guard Salaries.* Retrieved April 13th, 2014 from http://www1.salary.com/Security-Guard-Salary.html

Strobl, W. M. (1978). *Crime prevention through physical security*. New York: M. Dekker.

**Tang, Q., Bringer, J., Chabanne, H., Pointcheval, D. (2008). A Formal Study of the Privacy Concerns in Biometric-Based Remote Authentication Schemes. *Information Security Practice and Experience,* 56-70.