Global Information Assurance Certification Paper

Information Security Leadership

Ken Sweltz

In fulfillment of

SANS Security Essentials
GSEC Practical Assignment
Version 1.2e

June 16, 2001

Introduction

Many organizations have implemented sophisticated and redundant physical security mechanisms. This may include perimeter fences, surveillance cameras, armed guards, and employee badges. Proprietary information is shredded, sensitive materials are locked up during non-working hours, and random checks are conducted to ensure personnel are not leaving with unauthorized materials. These measures are usually very effective and the organization's leadership team knows they have exercised due care and diligence. However, individuals from this same leadership team may routinely leave their laptops unattended in hotel rooms where sensitive information could be unknowingly transferred from their hard drives. In other cases, patches and updates may not be properly applied to their critical servers and thus they become targets for unscrupulous individuals who can steal data or disrupt the organization's activities. In their management of information security, the leadership team is placing the organization at risk. This is not necessarily intentional irresponsibility on their part. In many cases it may be a failure to recognize or be properly informed of the threats and the appropriate responses to take. This is supported by a survey of computer security experts and managers at SANS 99 where they identified the second most prevalent management error that leads to security vulnerabilities security as managers who understand physical security but not the consequences of poor information security [10].

In this paper, I will examine some of the reasons for a lack of management awareness in dealing with information security; some possible dilemmas even informed management faces when trying to implement proper information security controls; and possible recourses for information security professionals to use to mitigate these problems. My discussion is primarily focused on organizations in the commercial sector.

Physical Security versus Information Security

It is easy to understand why management is more comfortable with physical security. In most cases they have been exposed to it all their lives. They left a secure hospital shortly after their birth wearing an identification bracelet and have been exposed to physical security procedures ever since. As children they watched their parents lock homes and cars, turn on outside lights for safety, and perhaps even had a family pet who served as a means of deterrence. Many of these individuals served as a patrol guards or hall monitors in grade school. They know that you significantly reduce the risk of theft by securing your wall locker. For those with military service, guard duty and physical safeguards were a routine experience. Physical security is something they can see and touch. The success of failure of implementation is easily observed.

Unfortunately, information security is not as easily understood. Many individuals on an organization's leadership team did not come of age exposed to computers, networks, and information security practices. They often do not have the technical background to intuitively understand the risks or controls. They hear the hype, but do not know what courses of action to take. Even if information security measures are implemented, they are unsure how to measure effectiveness and determine the all-important Return on Investment. In some cases, the failure to properly implement information security controls may not even be recognized. The Computer Emergency Response Team (CERT) at Carnegie Mellon has estimated that only 10 percent of attacks are detected [2]. Proprietary information can be taken from company servers without

their knowing the theft has occurred. It often takes a significant life experience such as an embarrassing defacement of a web site, a distributed denial of service attack that cause a loss of revenue, or theft of sensitive information such as credit card numbers before action is taken. This results in reactive versus proactive leadership which can lead to decisions made in the heat of the moment that may result in numerous failures to include:

- Not understanding the extent and source of an intrusion;
- Not putting proper protection mechanisms in place to prevent further damage;
- Not properly collecting forensics data to aid in prosecution of the perpetrators [3].

The Problem

There is mounting evidence that cyber attacks both by sophisticated hackers and script kiddies are on the rise. The following from the "2001 Computer Crime and Security Survey" conducted by the Computer Security Institute and Federal Bureau of Investigation confirms that there is a significant threat from computer crime and information security breaches. The results include:

- Eighty-five percent of respondents detected computer security breaches within the last twelve months;
- Sixty-four percent acknowledged financial losses due to computer breaches;
- Thirty-five percent of the respondents reported $377,828,700 in financial losses. This was a significant increase over the average annual total over the previous three years of $120,240,180;
- The most serious financial losses occurred through theft of proprietary information and financial fraud;
- Seventy percent of respondents cited their Internet connection as the most frequent point of attack. This is a rise from the 59% reported in 2000 [4].

There are estimates that 4,000 web sites are targeted for Distributed Denial of Service attacks each week. This includes attacks against Microsoft, the Central Intelligence Agency, the White House, and the Computer Emergency Response Team Coordination Center hosted by Carnegie Melon University [12].

The current cyber threat can take a variety of forms to include:

- Threat of Disruption. This can include disruptive viruses and denial of service attacks that could impact commercial communication flows such as banking transactions;
- Threat of Exploitation. This involves the compromise of sensitive or proprietary information and includes identity spoofing, credit card fraud, and information theft;
- Threat of Manipulation. This can be done for political or economic reasons or just for pure vandalism. It can be something simple such as the defacement of a web site or more serious such as the manipulation of financial and infrastructure data;
- Threat of Destruction. This involves exploits that access systems and cause data to be wiped out on hard drives or other data storage systems [2].

Because of these threats it is imperative that information security professionals and organizational leadership work together to understand the vulnerabilities and put proper security controls in place.

The Challenge

The challenge facing information security professionals is to ensure the organization's leadership understands what the information security risks are and what possible mitigation measures can be implemented to reduce those risks. Security professionals also need to make their leadership aware that absolute security is not achievable. Good security practices cannot eliminate risk; they can only be used to mitigate it [8]. There is also an inverse relationship between functionality and security controls; i.e., the more controls you put in place the less functional the system will be. Finally, the key is to achieve all of this in a proactive versus reactive manner.

The Dilemma

Even for a leadership team concerned about information security, it takes time for them to comprehend all the issues well enough to balance them against other competing interests in the organization [8]. They will be looking for ways to maximize profits and get the best Return on Investment. Management often believes that security is a drain on resources and has a difficult time equating money spent on security to improving the bottom line [8]. It can be difficult to have your leadership commit funds and resources to threats that may not materialize. You must be careful to not overplay your hand. There are numerous legitimate security concerns and a security professional should not get the reputation of "crying wolf". Your leadership could also have a false sense of security based on misperceptions. There are a number of myths that senior leaders may believe to be valid. These include:

- Firewalls provide adequate protection from the Internet;
- We have not been compromised so far so security is OK;
- Technology products alone can solve our security problems;
- We don't do anything to make us a target for attack [9].

Because the above myths have some degree of truth, it can be difficult to convince your leadership otherwise. The issue becomes using an appropriate approach to properly convey the right message to the decision makers so effective and efficient security controls can be put in place.

A Fix

Information security professionals need to be proactive in working with an organization's leadership. If there are breeches in security the information security professional will most likely be held accountable. Therefore it is good practice to document the recommendations you make and the action taken via formal written requests and memorandum for the record. Information security professionals and the leadership team often share the same goals but may be divided by divergent cultures that exist in an organization [6]. This can include differences in terminology and jargon. The information professional will use technical terms and concepts that could be unfamiliar to those on the leadership team. The leadership team will use business terminology

and legalese that may sound irrelevant or unimportant to the information security professional. Management will be looking for ways to maximize profits while the information security professional may want to implement security solutions without appreciating there are only finite funds available [6].

It is incumbent upon the security practitioner to try to bridge this cultural gap and work with management to ensure the organization is doing the right thing. There is no advantage in approaching your leadership in an adversarial or condescending manner. Although your leadership may not understand all the technical nuances involved, they are for the most part motivated and intelligence individuals who share your desire to protect the organization's assets.

The best way to reach your leadership and get a seat at their table is to be a leader yourself. This includes being prepared and conveying your message using the accepted professional standards of your organization. In most cases this will require a combination of written proposals and oral presentations. By having a thorough understanding of the issues you want to present, you will be able to convey your points in a confident and positive manner. This will increase the chances that they will be accepted for further consideration.

It is important to provide information in a form that is meaningful. Risk analysis is critical in determining what information security controls should be put in place. Organizations with the most effective risk analysis will be those that include a mix of individuals from business operations and those who have a technical understanding of the systems and security controls needed [5]. However, a recent survey indicated that more than 40% of organizations had no business unit participation in setting a value on information and digital resources [8]. This clearly needs to change in order to elevate information security concerns to a level where solutions will be implemented.

Risk management involves tradeoffs and coming up with a prioritized list that provides protection for your most critical assets. A good risk analysis will bring a degree of quantitative rigor to the process and help your leadership view information security from a business perspective.

When conducting risk analysis, a variety of issues such as policy, management, administration, and technology should be included to define an overall view of the information security posture of an organization. An information security risk analysis should be done in the following three sequential phases:

- Identify critical assets and the threats to those assets;
- Identify the vulnerabilities that expose those threats;
- Develop an appropriate protection strategy for the organization's mission and priorities [1].

Once a plan is put in place, it is important to periodically check it for applicability and make adjustments to meet the risks.

The General Accounting Office identified that the following risk management principles as best practice:

- Assess risk and define requirements;
- Establish a central focal point for your organization;
- Implement appropriate policies and controls;
- Promote awareness;
- Monitor and evaluate what is implemented [5].

When presenting the results of your risk analysis, the approach you use can make a big difference. This is especially the case when dealing with senior non-technical leaders. When providing examples of technology, use methods that will make the point. If you want to explain the concept of a "trace route" don't do it from the command line. Use a program such as NeoTrace to make your point with a graphical representation. In the first case you'll get glassy eyed stares. In the second case you will know they got it.

Analogies can be useful to help explain your key points to senior decision makers. These should not oversimplify the issues or make them trivial, but should be used to help get a point across that you might not otherwise be able to make. For example, one of the most important aspects of information security is to use a layered defense. Sometimes it can be difficult to explain why you need funding for firewalls, network intrusion detection systems, host intrusion detection systems, antivirus software, and vulnerability assessment tools. This may seem unnecessarily redundant. By using an example of the multiple layers of defense in a medieval castle, you can help illustrate your point.

It is also a good idea to have contingency plans prepared for anticipated threats that may get your boss's attention [8]. In many organizations vulnerabilities won't be addressed until they happen to a competitor or become headlines. If you are being proactive and have researched and prepared for these types of anticipated threats, you can not only get them approved when they now have management's attention but you will also gain credibility that will be useful for implementing other security controls.

It is important to gain early success when working with your management team. Go after low hanging fruit that will show that results are being made. This could include:

- Providing statistics on the number of probes that were successfully blocked;
- Running leadership approved password checking programs to identify weak passwords and having them corrected;
- Conducting employee awareness programs on security issues such as social engineering;
- Emphasizing your increased information security posture when attempting to win bids from other organizations that place a value on this.

Conclusion

In this paper, I examined some of the reasons for a lack of management awareness in dealing with information security; some possible dilemmas even informed management faces when

trying to implement proper information security controls; and possible recourses for information security professionals to use to mitigate these problems. Because of the current magnitude of the threat and the fact that everyone connected to the Internet is vulnerable, it is imperative that information security professionals and the organization's leadership work together proactively to put proper security controls in place. Once appropriate measures are implemented, individuals will need to be held accountable to ensure the measures are being properly applied. This will require periodic reassessments to verify that the measures are still effective and continual analysis to look for improved solutions and technologies to help combat changing threats. By establishing a dialogue with your business leadership, information security professionals will become leaders themselves and can forge a partnership to ensure that best practices are in place to keep their organizations secure.

List of References

1. Allen, Julia; Alberts, Christopher; Behrens, Samuel; Laswell, Barbara; Wilson, William. "Improving the Security of Networked Systems." URL: http://www.stsc.hill.af.mil/crosstalk/2000/oct/allen.asp

2. Borchgrave, Arnaud; Cillufo, Frank; Cardash, Sharon; Lederwood, Michele. "Cyber Threats and Information Security: Meeting the 21st Century Challenge" Center for Strategic and International Studies December 2000 (2000).

3. CERT Coordination Center. "Responding to Intrusions." URL: http://www.cert.org/security-improvement/modules/m06.html

4. Computer Security Institute. "2001 CSI/FBI Computer Crime and Security Survey." March 12, 2001 (2001).

5. General Accounting Office. "Information Security Management: Learning From Leading Organizations." May 1998 (1998).

6. Heiser, Jay. "Cultural Divide" Information Security Volume 4 Number 5 May 2001 (2001): 42.

7. Hernandez, Ernest D. "Network Security Policy." November 22, 2000. URL: http://www.sans.org/infosecFAQ/policy/netsec_policy.htm.

8. Prince, Frank. "Translating Security for Managers." Information Security Volume 4 Number 5 May 2001 (2001): 44 – 46.

9. Marsh, Jerry. "Myths Managers Believe About Security." January 25, 2001. URL: http://www.sans.org/infosecFAQ/start/myths.htm.

10. The SANS Institute. "The 7 Top Management Errors that Lead to Computer Security Vulnerabilities." 1999. URL: http://www.sans.org/newlook/resources/errors.htm (April 15, 2001)

11. Rowland, Carolyn. "Selling Security to Management in a Low Risk Environment." April 12, 2001. URL: http://www.sans.org/infosecFAQ/start/selling_sec.htm.

12. Stross, Randall. "Malicious Mischief" U.S. News & World Report June 18, 2001 (2001): 38.

Last Updated: May 23rd, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event