Information Security Fundamentals

By Cliff Riggs
June, 2003

Hill Associates offers a course that expands on this paper. For more information visit our website at *www.hill.com*.

Abstract

As recent events have shown, information security is an essential part of any organization's infrastructure plans. What, exactly, is information security? This paper defines information security, addresses the general goal of information security, provides an outline of implementation, and describes the tools available to implement information security.

Introduction

When designed correctly, information security is a process that adds value to an organization. Part of this process includes developing and implementing a security policy. We will describe what a security policy is, what it should do for an organization, and what it will not do. As we explain the process, we will explain the tools used to implement information security.

Information security implementation is a cyclical process that involves constant review and testing (Figure 1). Notice that the process includes a review component.

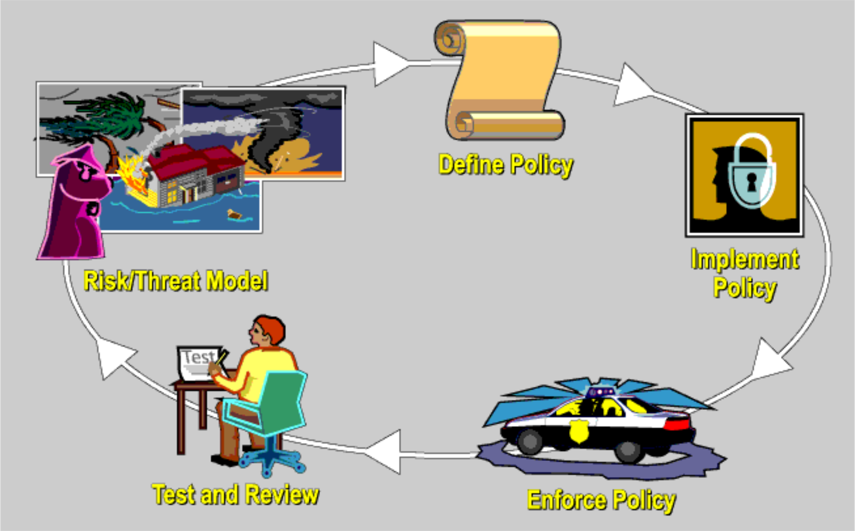

Figure 1: Information Security Process

Security Policy Is the Way

The first step to implementing information security is not based on technology. It involves developing a security policy, a short document (2–4 pages) that explains why you want to implement security. If you cannot find a reason to implement security (which I doubt), then do not. The security policy justifies the implementation of security measures. Do not implement security for its own sake; if you did, you would be letting technology drive the company, when the company should be driving the technology.

The policy should answer the questions below.

- *Why is security important to the company?*
- *How does security support the company's mission statement?*
- *What is the cost benefit of implementing a security policy?*
- *What are the consequences of not implementing and complying with the security policy?*

The cost benefit can be measured in numerous ways—tangible or intangible—such as increased productivity due to increases in network availability, compliance to local, state, or federal law, customer confidence, avoidance of poor publicity, integrity of data, and so forth.

In addition, the entire information security process must involve the technical staff and management so that the results are both technically feasible and enforceable (or the policy is useless).

The security policy will not change very often and will refer to other documents described below for implementation issues and other details. The contents of the other documents and ultimately the implementation must be measured against the security policy, so it is important to get it right. If the organization is doing things not mandated by the security policy (which describes why you are doing it in the first place), there is no benefit to the organization and resources are better focused elsewhere.

Security Standards: The What

The security standards document accompanies the security policy and describes what must be secured to comply with the policy. It might refer to other departments' documents (e.g., Human Resources requirements for confidentiality of employee data) or other standards and laws. It will identify an organization's assets, the risk to the organization if those assets are not protected, and the threats that must be protected against. When a risk or threat is identified, the company must decide whether or not to deploy countermeasures (i.e., steps to reduce the risk of an event having an effect) or insure against the risk; such measures should not cost more than the asset is worth.

An asset's worth is difficult to determine. One way is to estimate the replacement cost (the cost of downtime per hour x time to replace) To this cost, we add the cost of regenerating lost data. We would not use a quantitative value to determine an asset's worth when the asset must be secured to comply with law statutes or confidentiality expectations (e.g., the expectations of privacy of data held by government or military departments).

An asset is anything an organization requires to perform normal business operations. Some assets are listed below.

- People: *Expertise, corporate memory*
- Hardware: *CPU, drives, UPS, keyboards*
- Software: *OS, applications, source code, diagnostic software*
- Data: *Database, customer data, backups*
- Documentation: *Licensing, manuals*
- Supplies: *Ink, paper, media*
- Other: *Utilities*

The security standards should explicitly identify all assets critical to the business and the degree of threat and risk that they must be protected against. We do not need to build Fort Knox if only backups are required. The standards should also explain the consequences of noncompliance.

Security Procedures: The How

Once the security standards define what must be protected and the degree of protection, the security procedures are developed. This document must describe what must be done to ensure compliance to the other security documents and can include information such as network configuration templates, frequency of backups, firewall implementation, incident response, and frequency of log inspection. (Systems often record events—informational or critical—to a file called a log. This log could be on the same device that generates the message (e.g., a server, firewall, IDS, or router), or the log could be on a separate centralized server for correlation, prioritization, and notification of staff.)

The security procedures document is likely to be highly volatile as procedures are adapted to new threats or installed systems (and as the other described documents change).

Before finalizing the security documents, have legal counsel review them to confirm that legal requirements are met and that there is nothing left that would hold the company liable for its inclusion or exclusion. Even with careful preparation, some requirements might be interpreted ambiguously, so appoint a single person or committee to interpret the documents in case a question arises. The policy should clearly state that the right of interpretation lies with this appointed person or committee.

Implementing Information Security

Implementing information security is a complex process that must involve the whole organization to ensure success.

People

If all employees are not involved in implementing the security policy, it will likely fail. Education and training are crucial to successful security implementations.

Most employees today have a username and password that they need to protect. Logging off at the end of the day and at lunchtime are two ways to do this. Weak passwords are also a huge problem. Education is the key here; even better is staff involvement in the development of the security policy, participants will have a greater sense of ownership and responsibility, further ensuring its success.

Social engineering—where perpetrators masquerade as legitimate contractors, employees, or figures of authority and trick users into compromising information such as passwords—is also viewed as a weak link and can be addressed through education as well. Employees must understand that they should never give their passwords to other users, even if they say they are authorized, and they should report all incidents to their internal security hotline.)

Technology

Several technology options are available to help secure a network. Companies now need more than the traditional options of firewalls and filters. Intrusion detection systems (IDS) are becoming increasingly common as complements to firewalls; they monitor traffic in key places and log suspicious activity. Think of an IDS as a burglar alarm; passwords, firewalls, and filters are the locks on the network, and the IDS is the alarm system. An IDS does not stop a security event; it tells you about it. (Some of the more advanced IDSs can respond to an event with the intention of avoiding any losses, for example, resetting the suspicious TCP session or block suspicious traffic.)

Some of the technologies to help implement part of a security policy are defined below.

- Filter: *A router or firewall normally implements a filter—a set of rules that tells the device what to forward and what not to. Normally filtering involves inspecting the IP address and/or the UDP/TCP port number (i.e., the type* *of application). While effective, they are simple and easily circumvented. A filter is not a firewall by itself, but any firewall or security solution should use filtering.*

- Firewall: *A firewall connects two or more networks and manages traffic between them based on a set of rules. Much like a filter but more intelligent, the firewall more closely inspects a packet—its contents as well as its relation to other packets. It can also perform stateful inspection—inspect the contents of a stream of packets reassembled into the original message. A firewall does not expect to see any replies to unrequested messages and could filter such packets.*

- Proxy device: *A proxy device performs an action on behalf of a requesting device. For example, a web proxy requests web pages from the Internet on behalf of a user's PC, protecting the PC from the Internet or malicious websites. The proxy can filter content based on a policy. The proxy can also reply to the PC with the web page without retrieving it from the Internet again if someone else had already viewed the page, improving performance.*

- AAA: *Authentication, authorization, and accounting control access to resources on a network. Servers typically use the features to control access to server files, printers, and databases.*

- Authentication: *The act of verifying identity. Normally a password is used as proof; however passwords are traditionally not a robust method of authentication and are often augmented with a token authentication scheme, where users must know a PIN and also type in a random string generated by a small device or token. This is a better method of authentication as it relies on something you know (the PIN, which you can't lose but might be simple to guess) and something you have (a token, which you might lose but is useless without the PIN). An example of a token is shown in Figure 2.*

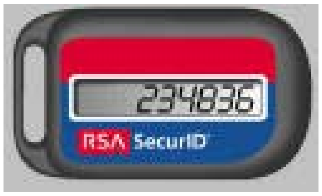

Figure 2. Token Example

- Authorization**:** *Once the system has verified you, what are you allowed to do? Different users will be authorized to perform different functions (e.g., delete files or read financial records).*

- Accounting: *The practice of tracking users' actions on the network. The granularity recorded depends on the goal. If the goal is to bill for resources (like a dial-up ISP), only the time connected will be recorded; if the goal is to catch a malicious, unauthorized user, all keystrokes might be recorded.*

- IDS: *The intrusion detection system can be a dedicated device connected to a network that inspects all traffic it sees on the network or a piece of software on a server that looks for suspicious activity (e.g., malformed packets, new files, deleted files, or unauthorized access). Network IDS devices report their findings back to a centralized IDS console that correlates*
  and prioritizes events and then takes some (e.g., page the IT staff or respond to the threat to thwart it).

- Encryption: *This process alters data so that it is unintelligible to unauthorized parties. What looks like gibberish to an unauthorized party is actually a meaningful message to the intended recipient. There are many ways to encrypt data: the simplest ways are easy to implement and easy for unauthorized users to unencrypt; some of the most complex ways are strictly controlled by the U.S. government. Often communication over a public infrastructure is encrypted, like credit card numbers sent over the Internet to buy goods.*

- VPN: *A virtual private network allows communication between two devices over a public (insecure) infrastructure, sometimes called a tunnel. A VPN often uses authentication to verify the source of the information being received and encryption to hide the information from all but the intended recipient. Common VPN technologies include IPSec and L2TP.*

- DMZ: *The demilitarized zone is part of a network that allows controlled access from the Internet; it is administered by a private entity. Web servers and mail servers are often placed here, as placing these devices on the internal network is not safe; allowing even controlled access to the internal network is a huge security risk.*

- Antivirus: *Antivirus protection typically includes both host-based and server-based protections. In addition to detecting and limiting the harmful effects of viruses, anti-virus software also provides important protection against other virus-like network payloads such as Trojans (backdoor programs) and worms (self-replicating programs).*

- Host/Server Security: *The proper, secure configuration of the operating system itself can help protect information. Commonly, important devices will be configured as bastion hosts by removing any software not essential to the server's operation. Likewise, directory permissions must be* *configured properly so that each user has the minimal rights required—least privilege—to perform his/her job functions. Finally, applying all software security patches in a timely manner can prevent many security incidents.*

Once all the components are in place, you must enforce the security policy. This is an ongoing process that is part of the security procedures. It involves auditing the network for ongoing compliance to the procedures as well as regularly inspecting logs for indications of non-compliance (e.g., unauthorized activity). You certainly want to realize any issues before they affect the business.

Incident Response

Recent events have shown that despite all the preparation and measures in place, security- related incidents will occur. Organizations must have a response plan to ensure the ongoing operation of the company. How an organization responds to an incident will vary depending upon the assets at risk and the intentions of the response. Below are two options.

- Pursue and prosecute: *Sometimes an organization's goal is to identify the culprit and prosecute. (This goal is likely to be at odds with recovering the system, as you will not want to let the intruder know that you are aware of his/her actions.) Consider the risk of further compromise, though, especially if you are allowing the perpetrator continued access so you can collect evidence.*

- Protect and proceed: *If the system is critical to the business and the chance of identifying the cause is small, the priority will be to systems recovery to ensure continuity of operation. It is difficult to find perpetrators who hide their identity by executing commands via a zombie or slave device that they have previously compromised and to punish perpetrators on another continent not subject to the same laws.*

The incident response plan should clearly define who has the authority to do what (e.g., bring systems down, talk to the media, notify management, or initiate chain of evidence procedures) and when. And, the incident response plan must be practiced. Too often, hasty decisions made under pressure lead to unexpected consequences, ranging from compromising further systems and delaying recovery to breaking the chain of evidence.

Immediately after an incident is the perfect time to review the policies, standards, and procedures. This is not an opportunity to apportion blame (except on the perpetrator) but to learn from the experience in an attempt to prevent future occurrences.

Risks and Threats

From what are we trying to protect our assets? A few examples of threats to network security are explained below.

- Virus: *A virus is code that self-replicates from file to file. Types of files infected include *.exe, *.doc, *.xls files. They can replicate slowly or quickly but only usually travel between computers as email attachments or on infected disks (i.e., as a result of human intervention). Examples include the Concept virus, Stoned.Michelangelo, and malicious MS Office macros.*

- Worm: *A worm is network-aware and copies itself from computer to computer via network shares or email packages. It propagates more quickly as a result, not requiring human help. Examples include SQL Slammer, "Melissa" (actually a virus and worm), AnnaKournikova, LoveLetter, Love Bug, and Explore Zip.*

- Trojan horse: *A Trojan horse is typically a non-replicating piece of software that a perpetrator installs covertly or by enticing an unaware user to run an otherwise benign program. The software then runs unaware to the computer user and can be used to launch other attacks, provide outside access, or feed sensitive information back to the perpetrator. Examples include BackOrifice, PKZIP.EXE Trojan horse, and NetBus.*

- Denial of service (DoS) attack: *These are attempts to consume resources on a network to the point where it cannot service legitimate users anymore. SQL Slammer consumed so much bandwidth across the Internet that even non-vulnerable devices and sites could not communicate across the network. SYN Flood attacks attempt to consume memory on a server to the point that the server cannot respond to individual user requests or crashes.*

- Distributed DoS attack: *While similar to DoS attacks, these are coordinated to originate from multiple (tens to thousands) of sources in an attempt to increase the effectiveness of the attack and/or hide the ultimate source. Often a perpetrator compromises multiple machines (zombies or slave devices) and instructs the zombies to launch the attack, so it is difficult to ascertain the ultimate source. Examples include attacks on CNN and Yahoo in the year 2000 and SQL Slammer in 2003.*

- Software bugs: *Faults in software cause a device to crash or allow unauthorized users to execute code on the compromised machine (e.g., SQL Slammer, 2003).*

- Interception of data *in transit compromises the contents.*

- Inside threats *from disgruntled employees threaten security.*

- Social engineering: *Perpetrators masquerade as legitimate contractors, employees, or figures of authority and trick users into compromising information such as passwords.*

- Acts of God: *These include floods, fire, hurricanes, and earthquakes.*

- Terrorist attacks and war.

- Systems failure *can compromise business operation just as deliberate attacks can. Maintain your equipment!*

Summary

Information security is not a one-time implementation; it is a complex process—one that involves developing a security policy, which then drives the development of security standards and procedures. Developing the policy must involve managerial and technical staff input to make it feasible and enforceable. Implementing the policy involves educating employees and invoking technology such as firewalls, IDS, encryption, and authentication. Competent execution of the policy includes creating an incident response plan and practicing the plan. Finally, ongoing compliance and return on investment involve post-incident review and constant auditing of the policy. In today's environment, a well-planned information security process is crucial; it can provide businesses real ROI, and sometimes, even save a business.

Bibliography

Books

Allen, Julia H. *The CERT Guide to System and Network Security Practices.* Boston: Addison-Wesley, 2001.

Harris, Shon. *CISSP All-in-One Exam Guide*. New York: McGraw-Hill, 2001.

Internet Resources

CERT Coordination Center. "CERT Security Improvement Modules." 19 June 2002. <http://www.cert.org/security-improvement/index.html> (7 March 2003).

CERT Coordination Center. “CERT Security Practices.” 9 July 2001. <http://www.cert.org/security-improvement/practices/practices.html> (7 March 2003).

Holbrook, P. and Reynolds, J., eds., Site Security Policy Handbook Working Group. “RFC 1244: Site Security Handbook.” July 1991. <http://www.ietf.org/rfc/rfc1244.txt?number=1244> (7 March 2003).

About Cliff Riggs

Cliff Riggs is a dedicated, knowledgeable, and passionate instructor, and his enthusiasm for teaching is clear. He challenges his students to think beyond the information in the given course materials-to consider real-world applications and related issues. Cliff's areas of technical expertise include TCP/IP, LANs, frame relay, routing and switching, security, e-commerce, and VPNs. Cliff also exhibits a passion for learning, as he holds several certifications: Cisco Certified Internetwork Expert (CCIE) #9413, Certified Information Systems Security Professional (CISSP), Certified Novell Administrator (CNA), Citrix Certified Administrator, Microsoft Certified Systems Engineer + Internet, and Microsoft Certified Trainer.

Cliff holds an M.Ed. from Johnson State College and is a member of the IEEE. Cliff has authored articles on IP addressing, BGPv4, IP multicasting, IP QoS, and MPLS. He is a contributing author to Telecommunications: A Beginner's Guide (McGraw-Hill/Osborne).

Prior to joining Hill Associates in 1999, Cliff was a high school teacher and a construction foreman. He owned and operated a construction company that built houses in the Vermont area, and worked as an event security guard for many national acts that have found their way to Vermont. Once turning his attention to computer networking, Cliff quickly established a name for himself as an independent consultant in the New England area.

About Hill Associates, Inc.

Hill Associates is a premier provider of training and marketing services in the field of telecommunications. For over 20 years, we have demystified the complex world of telephony, network security, and data communications for the most recognized players in the industry. Today we offer a variety of classes: classroom courses, hands-on workshops, self-directed e-learning, and virtual classroom e-learning. Our Marketing Services bring industry and subject matter experts to sales events, customer meetings, white papers, and Webinars.

At Hill Associates, our consultative approach addresses each client's unique needs and challenges. Whether it's executive consulting, training for field teams, network engineers, or corporate IT, or marketing programs designed to bring knowledge to prospects, Hill Associates delivers your solution. Visit us at www.hill.com and see what we can do for you.

Request for permission to use any portion of these materials should be sent to:

Hill Associates, Inc.
Attn: Copyright Coordinator
106 Highpoint Center
Colchester, VT 05446
USA

Phone	802-655-0940
Fax	802-655-7974
E-mail	info@hill.com
Web Site	www.hill.com

Although the mention, recommendation, or comparison of any name, product or service within this material is an expressed opinion by an industry expert, it should not be assumed as fact.

Hill
Associates®
an employee–owned company