Global Information Assurance Certification Paper

An Introduction to Information Security Concepts for the Non-Security Professional and Everyday Users

Mardel Shumake
July 23, 2004
GIAC-GSEC Practical Version 1.4b – Option 1

Abstract

There are volumes of technical documents and books about information security. Much of the writing about information security is fine for the security practitioner. However, for the non-security professional and the everyday user the information can be technically overwhelming. Security practitioners cannot expect everyone else to become security practitioners. Therefore security practitioners need to educate other users in information security. This document is an attempt to do educate users by providing them an introduction to information security.

Prelude

As an information technology professional it is easy for me to scoff at the lack of computer knowledge displayed by many users. Furthermore, as an information security practitioner, it is easy for me to ridicule other information technology professionals for their lack of understanding of information security. To have such an attitude is fine if I want to alienate myself and look like the infuriatingly condescending “Nick Burns, Your Company’s Computer Guy” from Saturday Night Live fame (NBC.com). I would prefer to squelch the know-it-all computer geek perception. In the book “Computer Security Incident Handling” Stephen Northcutt counsels us to share what we have learned while dealing with computer incidents (Northcutt, Introductory notes). This primer is an attempt to share, as non-technically as possible, some of the rudimentary aspects of information security.

Introduction

This introductory document should be beneficial to anyone using computers and concerned with information technology. Given our reliance on computers and the Internet that should include most of us. Hopefully security practitioners will find the information contained herein useful when trying to educate their users on information security. Also, most people would probably agree that an educated user is an asset to an organization rather than a liability.

With ever-increasing security risks and the availability of the Internet on nearly every desktop (Hall, p.1), information security has become a necessity at most organizations. Information security deals with what have become crucial assets to most organizations. An organization’s computer infrastructure and the information it contains are critical, valuable, and, unfortunately, vulnerable resources. Ongoing advances in technology and the growth of the Internet have increased the number of vulnerabilities associated with computer resources and the complexity of dealing with them (Fox, p.1).

Terminology

Like most professions the information technology community has developed its own jargon and uses a myriad of industry related terms. The information technology community and its sub-community, the information security community, are relatively young compared to other professional communities. Some of its definitions are short-lived and terms are constantly evolving to meet this rapidly growing industry. Even within the information technology community terms may vary from one sub-community to another. For instance the term "socket" may mean one thing to an information technology professional that specializes in writing computer programs and another thing to a networking specialist.

Even though these terms are constantly changing and sometimes leave users at all levels confused the reader needs some consistency in terminology, at least for the scope of this primer. The terms given below should help the reader without overwhelming them with technical jargon. Most of the definitions are deliberately simplistic and would not be satisfactory for professional information technology workers or security practitioners. However, they should be sufficient for a rudimentary information security primer.

Useful Terms

Hard Copy – Paper or printed copy of data.
Data – Distinct pieces of information (Webopedia.com). [1]
Denial of Service – When a resource such a network, computer, or disk drive is so overwhelmed with activity it can't perform properly.
Destination – The computer intended to receive data.
End User – See User.

Enterprise – Encompassing the overall scope of an organization.

Enterprise Level – Measures implemented or enforced at the highest point of organization or system hierarchy.
Firewall – A system designed to prevent unauthorized access to or from a network. (Webopedia.com)[2] Access is based on the source and destination of network packets.
Locking Screen or Login Screen – This is "screen" or interface that force authorized users to authenticate who they are before using a computer or a computer application.

Information Technology - General term used to describe technologies that help produce, manipulate, store, communicate, or disseminate information. (ucdavis.edu)[3]

Internet – Even though there are definite physical aspects to the Internet, the Internet is more of a concept than an established and concrete fixture. At its most fundamental level that concept is a global network of computers.

---

[1] Webopedia.com. http://www.webopedia.com/TERM/d/data.html.
[2] Webopedia.com. http://www.webopedia.com/TERM/f/firewall.html.
[3] Ucdavis.edu. http://iet.ucdavis.edu/glossary/#i.

Network – A group of two or more computer systems linked together. (Webopedia.com) [4]

Operating System – Software that performs and controls the basic hardware of a computer. The operating system is responsible for getting input from the user such as the user typing on a keyboard. In turn the operating system "tells" the computer how to respond.

Network Packet – A grouping of information that is sent through a network.

Personal Firewall – An application that is installed, often times by the end user, on a local computer. This application is designed to prevent unauthorized access to or from the local computer.

Source – The computer that is sending data over a network.

Storage Media – Magnetic or optical means of storing data.

System Administrator – Someone who is responsible for maintaining a multi-user computer system. (Webopedia.com)[5]

User – Someone authorized to access and utilize a computer and/or network resource.

Anti-virus software – A computer application designed to detect and/or prevent a computer from becoming infected with a virus.

Defining Security

Security can be defined as "the quality or state of being secure: as in freedom from danger" (Whitman and Mattord, p.9). Whitman and Mattord point out that successful organizations have multiple layers of security including:

- Physical security protects physical items from theft, unauthorized access and use.
- Personal security protects the individual or group of individuals who are authorized to access the organization and its operations.
- Operations security protects the details of a particular operation or series of activities.
- Communications security protects an organization's communications media, technology, and content.
- Information security protects the systems and hardware that use, store, and transmit that information (Whitman and Mattord, p.9).

Security practitioners recognize that even though users often see security measures as security solutions, they are, in fact simply obstacles to would be attackers. Implementing the various layers of security in a unified system helps to assure maximum effectiveness of security measures.

[4] Webopedia.com. http://www.webopedia.com/TERM/n/network.html.
[5] Webopedia.com. http://www.webopedia.com/TERM/s/system_administrator.html.

Because of the complexities involved in implementing the various layers of security it is often necessary to compartmentalize the layers. An organizations public safety department may oversee physical security while the information technology department oversees implementation of computer security. However, the two departments must communicate with one another and ensure that neither layer of security goes undone.

Even though users may become involved at any layer of security this primer will focus mainly on physical security and information security at the user level. It is beneficial for all users to be aware of the other layers of security. This should give users an idea of the complexity and breadth of responsibilities faced when implementing security measures.

By reporting an unsecured server room door, reminding other users to logout of their computers when they leave the office, or finding out why a stranger is wondering around the work area, users can help ensure information security. All users should remind one another that is everyone's responsibility.

Physical Security

As mentioned earlier physical security is usually associated with theft and unauthorized access. Even if an organization has strategically placed security cameras, information security personnel can't be in all places at once. Users are responsible for locking their offices, using locking screen savers, and not leaving sensitive information, such as passwords, lying about.

An organization can install all kinds of technological security measures such as firewalls. However, this does little good if a user or system administrator fails to lock the room in which the organization's server is kept and the server is stolen. Security measures are weakened when one layer of security is applied and another is left undone. In a case where a firewall has been installed and a door left unlocked, information security has been applied but physical security has been neglected.

Information Security

Many information security books, articles, and web sites discuss an information security model known as the CIA model. Even though additional goals have been added to this model and implementation of the model varies from source to source, three main tenets are generally present. CIA stands for Confidentiality, Integrity, and Availability. These are considered the core elements information security. The CIA model is sometimes referred to as the CIA triangle. A triangle is an apt description of the basic CIA model. If any part of the CIA model is missing the model is incomplete and the triangle cannot be formed.

Confidentiality

Guarding against the intentional or unintentional unauthorized disclosure of information is an essential part of good information security (Russell, p.1). Users, especially managers and administrators, should ensure that proper steps are taken to guarantee the confidentiality of the information they are responsible for.

Work with security personnel to determine the sensitivity of information and the level of protection required (Lawrence, p.4).

Two oft-neglected areas of information confidentiality are the storage and disposal of hard copies of information. Printed copies of sensitive information should be stored in a manner that protects them from theft and that limits access to the copies to personnel authorized to view such information. Ensure that printed copies of sensitive information, including carbon copies or duplicates, are disposed of in a manner that prevents the material from falling into inappropriate hands. Many organizations require the burning or shredding of hard copies of sensitive information.

Another ignored aspect of information confidentiality is the retirement of storage media that contains or has contained sensitive data. Storage media should not simply be tossed in the trash or given away. Even if the media has been erased it may still contain residual information.

Users should check with their organization about the storage and disposal of printed copies of sensitive information and the retiring of storage media. If the organization does not have procedures in place for handling these situations the user should point out that the organization is responsible for ensuring the confidentially of all sensitive information.

Integrity

Integrity ensures that unauthorized personnel or processes or authorized personnel or processes don't make unauthorized modifications to data or systems (Russell, p.1). Integrity can be assured by using programs and procedures that report the access to and modification of data or systems (Lawerence, p.5).

Users can help guarantee the integrity of data and systems by making only the changes that they are authorized to make. Also, they should document and report every change that they make.

Availability

Many organizations try to provide 24x7 access to the organization's computing and networking resources. Most people would agree that not being able to send or receive email or access your organization's web site are more than just mere inconveniences. Today sending and receiving email is an essential aspect of our job.

Ensuring the availability of computer and network resources is often considered the responsibility of information security departments. However, there are simple practices that end users can do to help ensure availability of computer and network resources. Most users have either encountered a computer virus or worm or know someone that has. Today viruses and worms are often distributed via email attachments. One of the ways that a user can help ensure the availability of computer and network resources is by not opening email attachments. The distribution of viruses and worms is often triggered when a user opens an infected email attachment. The virus or worm is then "passed"

around the organization's network or through email to infect other user's computers. Eventually this can stress an organizations computing and networking resources to the point that these resources become unavailable.

Internal Hurdles to Security

Even though organizations face external hurdles to implementing security it is often the internal hurdles that weaken or prevent security. There is often little an organization can do to prevent attackers from outside the organization from "attempting" to breach the organization's security.

Over Tasked and Understaffed Information Technology Departments

Many information technology departments are understaffed and suffer from a shortage of properly trained information security personnel. There is an even greater lack of people properly trained in responding to and handing computer security incidents. It is not uncommon for someone with a modicum of information technology experience to be assigned the job information security and also the job of incident handling.

Lack of Awareness, Training, and Education

Organizations often lack proper security awareness, training, and education programs. Sometimes management assumes that information technology and/or security departments are educating employees. However, anyone involved in educating users, will quickly tell you that even if the information technology department offers awareness and training classes few people attend the classes. Users are already busy and their departments are reluctant to release them for classes. Organizations need to realize that security is everyone's problem and make awareness and training programs mandatory.

Users are Compelled to do Dumb Things

Even when users are aware of security issues they still seem compelled to do dumb things.

In an online magazine article the columnist points out how one user, described as a supervisor and a very intelligent and knowledgeable one at that, was most insistent about opening a questionable email attachment. The attachment was not from an internal source and was of a dubious nature. The manager asked whether or not she should open it and was concerned that she might miss something important if she didn't open it. The article goes on to say that whoever was helping the user "practically had to nail her hands to the desk" to keep her from opening the attachment. When the user was asked if she opened everything, (apparently mail), she got at home, she answered, "Yes." When asked, "why?" the user couldn't answer the question (Dvorak, p.1).

The author went on to suggest, rather tongue-in-check, that users suffer from obsessive compulsive disorder, or OCD, or that the user was simple compelled to open the attachment no matter the consequences.

Misunderstanding Security Related Technology

Over the years vendors have pushed technologies that are supposed to “solve” an organization’s security problems. These vendors have advertised firewall, intrusion detections systems, and one warning system or the other that either alert us to or prevent security violations. The management of many organizations has bought into the advertising ploys of vendors without taking into account the rapidly changing environment of information technology.

Also, managers and information technology departments often don’t know how to deploy and implement security related technology. Training security is often expensive and organizations do not dedicate funding for such training.

Users sometimes think that if their organization has a firewall they are safe from everything.

All users need to recognize that a firewall is simply a measure of security that controls network traffic. A firewall does not guard against viruses.

Users are lulled into thinking that they will never get a virus because their organization has an enterprise level anti-virus application and also requires them run anti-virus software on their computer.

Anti-virus applications work by comparing the contents of a file with what are know as virus signatures. These are pieces of code, snippets of text, or phrases that are known to exist in a given virus. Since “bad guys” are constantly re-creating old computer viruses and introducing new ones sooner or later viruses may get by an organization’s virus protection barriers.

Another internal problem faced by organization when they try to implement security measures is that users lock their office door but don’t use a locking screen saver or logout of their computer.

A common complaint heard by security practitioners is that someone has used someone’s computer when they were out of the office even though the office was locked. Many organizations are lax about handing out “master” keys to office buildings. Cleaning crews, security personnel, outside contractors, are just a few of the people that often end up with such keys.

Some users believe that because their organization has a Security Information Officer or security staff the user is not responsible for information security. This is an all too common belief of users and even the management of organizations. In the opening letter of “The National Strategy to Secure Cyberspace” President George Bush points out that computer security requires a “coordinated and focused effort from our entire society” (Department of Homeland Security, Opening Letter).

Security Incidents

The best way to “handle” an incident is to stop it from happening. (Northcutt) Users can help prevent security incidents by following their organization’s acceptable use and security policies.

No amount of prevention will stop all attacks or security violations. Eventually organizations will have to deal with a security incident. Security practitioners will tell you that it is not a matter of if an incident will occur but when it will occur. Conventional computer security practices recommend that organizations develop a plan to handle incidents. Incident handling books and documents talk about forming teams to deal with these attacks and violations.

Incident handling or incident response as it is often called is. For this primer we will use the term incident handling because “handling” implies more than just “responding” to an incident. Incident handling is a multifaceted discipline that usually requires a coordinated effort from several different operational units of an organization. Coordination between the end user, help desk workers, security professionals, human resources personnel, etc. may find themselves involved in a computer security incident (Mandia, Prosise, and Pepe, p.13).

Users should generally leave incident handling to the people assigned to deal with incident handling. However, users still play a critical role in the incident handling process. Users should be taught how they should react to an incident and who to contact when an incident takes place.

Users need to recognize the difference in a “normal” event and an event that has become an incident.

Events

An event is any observable occurrence in an information system or network (Grance, Kent, and Kim, p.2-1). Saying that an event is observable does not mean that someone has to be watching the event take place in real-time. Observable also may, and often does, mean that the event has been recorded or logged. Events include such activities as the boot process of a computer, a user sending or receiving email, a firewall blocking a connection attempt, and a user logging into a computer. These events are “normal” and happen on most networks and computers.

Sometimes users become alarmed when they see that their personal firewall has blocked an attempted connection. However, remember that your firewall has done its job. It might not be a bad idea to contact someone at the enterprise level and let them know that your firewall has blocked an attempted connection. However, users need to realize that when their personal firewall blocks an unauthorized connection it has prevented a compromise.

Incident

An Incident is an adverse event in an information system or network (Northcutt, p 43). Incidents include such adverse events as unauthorized access to a computer or network, release of malicious code, a virus infection, and a denial of service.

Panic is an Enemy of the Security Practitioner and of the Incident Handler

No one should panic during an incident. Users should remain calm and contact their security department or representative. Often times users and even seasoned system administrators will panic and begin rebooting a computer that they suspect of being involved in an incident.

The act of rebooting the computer often destroys information that could have been valuable to the incident handler. Once the system is rebooted that information or evidence is gone forever.

Record and Report Everything

Since users are more often than not using the computer when they begin to suspect that an incident has taken place they should record and report everything they see. Such things as a computer running slow or sluggish for no apparent reason, the users hard drive all of a sudden fills up, etc. are events that may indicate an incident.

Communication

Earlier in the primer a few terms where presented. Security practitioners and incident handlers would appreciate your knowing and using these terms. However, if you are an “average” user don’t get too wrapped up in understanding the numerous of terms associated with information technology.

When you are explaining what happened during an incident use your own language. Be clear and as concise as possible. At the same time remember that in the world of computers, especially when it comes to security and incidents, “nothing just happens.” To the person(s) handling the incident every detail is potentially important. If you think of something “strange” that happened several days ago report it.

Concluding Remarks

This has been an introduction to information security concepts for non-security personnel and users. Readers are urged to continue to educate both themselves and others in information security.

References

Department of Homeland Security, The National Strategy to Secure Cyberspace. February 2003. http://www.dhs.gov/interweb/assetlibrary/National_Cyberspace_Strategy.pdf

Fox, Scott. Collection and Dissemination of Computer and Internet Security Related Information (Alerts, Advisories, Incident Notes, Vulnerability Notes, Summaries, and other Bulletins). SANS.org. August 21, 2001. http://www.sans.org/rr/papers/index.php?id=637.

Grance, Tim, Kent, Karen, and Kim, Brian. Computer Security Incident Handling Guide, Special Publication 800-61, National Institute of Standards and Technology, January 2004. http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf.

Hall, Mary (Missy). Implementing a Computer Incident Response Team in a Smaller, Limited Resource Organizational Setting. SANS.org. March 15, 2003. http://www.sans.org/rr/papers/index.php?id=1065.

Lawrence, Patti. Acceptable Use: Whose Responsibility Is It? SANS.org. March 20, 2002. http://www.sans.org/rr/papers/index.php?id=3.

Mandia, Kevin, Prosise, Chris, and Pepe, Matt. Incident Response and Computer Forensics, 2nd Edition. New York: McGraw Hill/Osborne, 2003.

NBC.com. Saturday Night Live. http://www.nbc.com/Saturday_Night_Live/bios/Jimmy_Fallon.html

Northcutt, Stephen. Computer Security Incident Handling, Version 2.3.1. United States of America: SANS Press, March 2003.

Russell, Chelsa. Security Awareness – Implementing an Effective Strategy. SANS.org. October 25, 2002. http://www.sans.org/rr/papers/index.php?id=418.

Whitman, Michael E. and Mattord, Herbert J. Principles of Information Security. United States of America: Course Technology, 2003.

Last Updated: May 23rd, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 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 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	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Atlanta SEC401	Atlanta, GA	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