Teaching The Human Side of Information Security

Herbert J. Mattord, CISSP
Kennesaw State University

March 2004
The Need For Information Security
Information Security

Information security is the systematic protection of information and its critical elements, especially the systems that use, store, and transmit that information.

It is the protection of the confidentiality, integrity and availability of information while in transmission, storage or processing, through the application of policy, technology, and education and awareness.
The Great Wall
Critical Characteristics Of Information

The value of information comes from the characteristics it possesses:

– Availability
– Accuracy
– Authenticity
– Confidentiality
– Integrity
– Utility
– Possession
Controlling Information Security Risk

Information Security risks can be controlled by using one of three types of controls (also known as safeguards):

- Policy effectively developed, applied and enforced
- Security Education Training and Awareness (SETA) programs developed, adequately funded and consistently applied
- Technical solutions applied using a thorough blueprint and consistently applied
Information Security

Information security (InfoSec) is unlike any other aspect of information technology, an arena where the primary mission is to ensure things stay the way they are. If there were no threats we could focus on improving systems resulting in vast improvements in ease of use and usefulness.
What is InfoSec?

- Information security
- Network security
- Policy
- Computer & data security
- Management of information security

Teaching the Human Side of Information Security
InfoSec is Also Risk Control

THREAT

ATTACK VIA VULNERABILITY

CONTROLS

RESIDUAL RISK

LOSS
Threats

Management must be informed of the various kinds of threats facing the organization.

A threat is an object, person, or other entity that represents a constant danger to an asset.

By examining each threat category in turn, management effectively protects its information through policy, education and training, and technology controls.
Threats

The 2003 CSI/FBI survey:

♦ 530 specific respondents from many industries and sizes of companies (note all were self selected)
♦ 56% of respondents reported unauthorized use in 2002 down from average of 59% over the previous seven years of the survey
♦ Overall number of significant incidents remained roughly the same as previous year
♦ Theft of proprietary information caused the greatest financial loss among survey respondents
♦ The second most expensive computer crime among survey respondents was denial of service
♦ Virus incidents (82 percent) and insider abuse of network access (80 percent) were the most cited forms of attack or abuse
Threats to Information Security

♦ Acts of Human Error or Failure
♦ Compromises to Intellectual Property
♦ Deliberate Acts of Espionage or Trespass
♦ Deliberate Acts of Information Extortion
♦ Deliberate Acts of Sabotage or Vandalism
♦ Deliberate Acts of Theft
Threats to Information Security

♦ Deliberate Software Attacks
♦ Deviations in Quality of Service from Service Providers
♦ Forces of Nature
♦ Technical Hardware Failures or Errors
♦ Technical Software Failures or Errors
♦ Technological Obsolescence
## Threats, Threat Agents, Exploits, Vulnerabilities and Attacks

<table>
<thead>
<tr>
<th>Threat</th>
<th>Deliberate Software Attack</th>
<th>Forces of Nature</th>
<th>Information Extortion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat-Agent</td>
<td>Virus or Worm in an Email Attachment</td>
<td>Hurricane</td>
<td>Blackmailer</td>
</tr>
<tr>
<td>Vulnerability</td>
<td>Outlook runs programs with few authentication steps</td>
<td>Building failure</td>
<td>Buffer overrun in web server</td>
</tr>
<tr>
<td>Exploit</td>
<td>User is sent a program to install a zombie</td>
<td>Hurricane at our location</td>
<td>Script to gain control of web server</td>
</tr>
<tr>
<td>Attack</td>
<td>Zombie used for indirect attack against others</td>
<td>Hurricane takes roof</td>
<td>Steal file of Credit card numbers</td>
</tr>
<tr>
<td>Loss</td>
<td>Image, possible liability</td>
<td>Storm damage and downtime</td>
<td>Image, liability, market share</td>
</tr>
</tbody>
</table>
## Threats to Information Security

<table>
<thead>
<tr>
<th>Threat</th>
<th>Mean</th>
<th>Std. Dev</th>
<th>Weight</th>
<th>Weighted Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Deliberate Software Attacks</td>
<td>3.99</td>
<td>1.03</td>
<td>546</td>
<td>2178.3</td>
</tr>
<tr>
<td>2. Technical Software Failures or Errors</td>
<td>3.16</td>
<td>1.13</td>
<td>358</td>
<td>1129.9</td>
</tr>
<tr>
<td>3. Act of Human Error or Failure</td>
<td>3.15</td>
<td>1.11</td>
<td>350</td>
<td>1101.0</td>
</tr>
<tr>
<td>4. Deliberate Acts of Espionage or Trespass</td>
<td>3.22</td>
<td>1.37</td>
<td>324</td>
<td>1043.6</td>
</tr>
<tr>
<td>5. Deliberate Acts of Sabotage or Vandalism</td>
<td>3.15</td>
<td>1.37</td>
<td>306</td>
<td>962.6</td>
</tr>
<tr>
<td>6. Technical Hardware Failures or Errors</td>
<td>3.00</td>
<td>1.18</td>
<td>314</td>
<td>942.0</td>
</tr>
<tr>
<td>8. Forces of Nature</td>
<td>2.80</td>
<td>1.09</td>
<td>218</td>
<td>610.9</td>
</tr>
<tr>
<td>9. Compromises to Intellectual Property</td>
<td>2.72</td>
<td>1.21</td>
<td>182</td>
<td>494.8</td>
</tr>
<tr>
<td>10. Quality of Service Deviations from Service Providers</td>
<td>2.65</td>
<td>1.06</td>
<td>164</td>
<td>433.9</td>
</tr>
<tr>
<td>11. Technological Obsolescence</td>
<td>2.71</td>
<td>1.11</td>
<td>158</td>
<td>427.9</td>
</tr>
<tr>
<td>12. Deliberate Acts of Information Extortion</td>
<td>2.45</td>
<td>1.42</td>
<td>92</td>
<td>225.2</td>
</tr>
</tbody>
</table>
Attacks

An attack is the deliberate act that exploits vulnerability

It is accomplished by a threat-agent to damage or steal an organization’s information or physical asset

– An exploit is a technique to compromise a system
– A vulnerability is an identified weakness of a controlled system whose controls are not present or are no longer effective
– An attack is then the use of an exploit to achieve the compromise of a controlled system
Attacks

Back Doors
Brute Force
Buffer Overflow
Denial-of-service (DoS)
Dictionary
Distributed Denial-of-service (DDoS)
Hoaxes
IP Scan and Attack
Mail-bombing
Man-in-the-Middle
Mass Mail
Password Crack
Simple Network Management Protocol
Sniffers
Social Engineering
Spam
Spoofing
Timing Attack
Unprotected Shares
Virus, Worm, Trojan
Web Browsing
People

“People are the weakest link. You can have the best technology; firewalls, intrusion-detection systems, biometric devices ... and somebody can call an unsuspecting employee. That's all she wrote, baby. They got everything.”
Security is a People Problem

Money may be the root of all evil, but people are the root of all problems. People, who are all fallible, are usually recognized as one of the weakest links in securing information. The problem is: no matter how much work is placed in the protection of information, it only takes one misguided soul to completely defeat all efforts.
Top Threats to InfoSec

Deliberate Software Attacks
  – viruses – created by people, propagated by people
  – DOS – caused by people

Technical Software Failures or Errors
  – Programming glitches – caused by people

Act of Human Error or Failure
  – people errors, people failures

Deliberate Acts of Espionage or Trespass
  – Hacking and sniffing – by people

Deliberate Acts of Sabotage or Vandalism
  – Web page defacements, trashing hardware/software – by people
Sun Tzu

“Know the enemy and know yourself; in a hundred battles you will never be in peril. When you are ignorant of the enemy but know yourself, your chances of winning or losing are equal. If ignorant both of your enemy and yourself, you are certain in every battle to be in peril.”
The Solution

The solution to the human problem is:

♦ Planning – to deal with the problems
♦ Policy – to inform
♦ Security Education, Training and Awareness Program: SETA – to educate…
♦ Law – to enforce
♦ And yes, technology…
Planning

Security Planning
– Strategic, Tactical & Operational

Contingency Planning
– Incident Response Planning
– Disaster Recovery Planning
– Business Continuity Planning
Policy

- Security Program Policy
- Issue-Specific Security Policy
- System-Specific Security Policy

Policy MUST be:
- Created,
- Distributed
- Read
- Understood
- Agreed-to
Policies

Sanctioned by organizational most senior management

 Built from sound policy, requiring that policy be established first.

 Detailed steps, which when followed, meet the requirements of standards.
The purpose of computer security awareness, training, and education is to enhance security by:

- improving awareness of the need to protect system resources;
- developing skills and knowledge so computer users can perform their jobs more securely; and
- building in-depth knowledge, as needed, to design, implement, or operate security programs for organizations and systems.
SETA Awareness Components
Training

The purpose of training is to teach people the skills that will enable them to perform their jobs more securely. This includes teaching people what they should do and how they should (or can) do it. Training can address many levels, from basic security practices to more advanced or specialized skills. It can be specific to one computer system or generic enough to address all systems.
Education

Security education is more in-depth than security training and is targeted for security professionals and those whose jobs require expertise in security. Techniques. Security education is normally outside the scope of most organization awareness and training programs. It is more appropriately a part of employee career development.

Security education is obtained through college or graduate classes or through specialized training programs. Because of this, most computer security programs focus primarily on awareness and training.
The Human Firewall

“a Human Firewall is defined as a comprehensive approach recognizing that information security critically depends on people in order to be effective.

The Human Firewall acknowledges that every worker who comes in contact with sensitive, valuable and confidential information must participate as a team to make information security more effective.
The Human Firewall Manifesto

“Clearly, information security has to be improved upon if we are to properly protect the valuable information assets that drive our economy.

Technology alone can't solve the challenges of Information Security.

The way we do business now often compromises Information Security.

“It's time to change the way we think about Information Security---and the way we manage it.

…it is essential that we broaden our definition of information security to include the people who actually make it happen…”
Albert Einstein

Only two things are infinite, the universe and human stupidity, and I'm not sure about the former.

Problems cannot be solved at the same level of awareness that created them.
Information Security Technology

Information security - A discipline that relies on people, policy, education, training, awareness, procedures, and technology to improve the protection of an organization’s information assets.

Technical solutions can maintain:
- Confidentiality of information
- Integrity of information
- Availability of information
Areas of Technical Control

Firewalls
Dial-up Protection
Intrusion Detection Systems
Scanning and Analysis Tools
Cryptography
Access Controls
Others
Teaching Information Security

- You may have seen Dr. Whitman’s presentation (scheduled for yesterday)
- It outlined a pragmatic and pedagogically sound approach to developing curriculum
- In a nutshell, align learning outcomes with constituent needs and then find ways to bring students along for the journey
Learning Outcomes

♦ Curriculum should be founded upon sound learning outcomes
♦ Generating learning outcomes is a collaborative effort with many voices (constituencies) that deserve to be heard
♦ Identify the extent to which the student is expected to learn the each component of each knowledge area
Creating InfoSec Courses and Programs

Courses and programs should be created in ways that:

– Involve all critical stakeholders
– Create employable students or students who can advance academically
– Capitalize on available resources (faculty, classrooms, labs)
– Support local / state / national program objectives like the National Strategy to Secure Cyberspace
Resources Needed to Support ISA Curricula

Classrooms
Texts
Labs
Internships / Coops
Business Partners / Clients
Resources To Help Build Curricula

Local
- Department / College / University
- Advisory Boards
- Business Partners

Regional
- Conferences (like InfoSecCD 2004 at KSU in September)

National
- NIST and other documentation resources
- NSA Centers of Excellence program
- NSF and other Grants
Supplemental Materials

NIST Self-Assessment

NSTISSC Documentation

National Strategy to Secure Cyberspace

Textbook publishers
– Course Technology
http://www.course.com
Section I – Introduction
1. Introduction to Information Security

Section II – Security Investigation Phase
2. The Need for Security
3. Legal, Ethical and Professional Issues in Information Security

Section III – Security Analysis
4. and 5. Risk Management

Section IV – Logical Design
6. Blueprint For Security
7. Planning for Continuity

Section V – Physical Design
8. Security Technology

Appendix – Cryptography
9. Physical Security

Section VI – Implementation
10. Implementing Security
11. Security and Personnel

Section VII – Maintenance and Change
12. Information Security Maintenance
Section I – Introduction
1. Introduction to Information Security

Section II – Security Investigation Phase
2. The Need for Security
3. Legal, Ethical and Professional Issues in Information Security

Section III – Security Analysis
4. Risk Management: Identifying and Assessing Risk

Section IV – Logical Design
5. Planning For Security

Section V – Physical Design
6. Security Technology: Firewalls and VPNs
7. Security Technology: IDS, Access Controls & Tools
8. Security Technology: Cryptography
9. Physical Security

Section VI – Implementation
10. Implementing Security
11. Security and Personnel

Section VII – Maintenance and Change
12. Information Security Maintenance
Table of Contents
Section I - INTRODUCTION
1. Introduction to Management of Information Security
Section II - PLANNING
2. Planning for Security
3. Planning for Contingencies
Section III - POLICY AND PROGRAMS
4. Security Policy
5. Developing Security Programs
Section IV - PROTECTION
7. Risk Assessment
8. Risk Management and Control
9. Protection Mechanisms
Section IV - PEOPLE AND PROJECTS
10. Personnel and Security
11. Law and Ethics
12. Security Project Management
Table of Contents

Theme 1 - Scanning & Enumeration
Theme 2 - OS Vulnerabilities
Theme 3 - Firewalls and IDSs
Theme 4 - InfoSec Maintenance
Theme 5 - InfoSec Mgt Tools
Theme 6 - OS & File Systems
Theme 7 - Computer Forensics

Support Files:
Common Utilities
Representative Answers
Lab Configuration and Setup

Michael E. Whitman, Herbert J. Mattord & Dave M. Shackleford © 2005 Course Technology
Table of Contents

1. Security Overview
2. Authentication
3. Attacks and Malicious Code
4. Remote Access
5. E-mail
6. Web Security
7. Directory and File Transfer Services
8. Wireless and Instant Messaging
9. Devices
10. Media and Medium
11. Network Security Topologies
12. Intrusion Detection
13. Security Baselines
14. Cryptography
15. Physical Security
16. Disaster Recovery and Business Continuity
17. Computer Forensics and Advanced Topics

Cisco Learning Institute,
Boswell, Calvert, Campbell
© 2003
Course Technology
ISBN: 0-619-12017-7
Table of Contents

1. Foundations of Network Security
2. Designing a Network Defense
3. Risk Analysis and Security Policy Design
4. Choosing and Designing Firewalls
5. Configuring Firewalls
6. Strengthening and Managing Firewalls
7. Setting up a Virtual Private Network
8. Intrusion Detection: An Overview
9. Intrusion Detection: Preventive Measures
10. Intrusion Detection: Incident Response

Appendix A: SC0-402 Objectives
Appendix B: Security Resources
Chapter 1 - Computer Forensics as a Profession
Chapter 2 - Computing Investigation Processes
Chapter 3 - Microsoft Operating Systems, Boot Processes and Disk Structures
Chapter 4 - Macintosh and Linux Operating Systems, Boot Processes and Disk Structures
Chapter 5 - The Investigator’s Office
Chapter 6 - Current Computer Forensics Tools
Chapter 7 - Digital Evidence Controls
Chapter 8 - Crime/Incident Scene Processing
Chapter 9 - Data Acquisition
Chapter 10 - Computing Forensics Analysis
Chapter 11 - Email Investigations
Chapter 12 - Graphic Image Recovery
Chapter 13 - High Tech Reports
Chapter 14 - Expert Witness Overview
Appendix A - Recommendations for Computing Investigations
Thank You For Your Time