Choosing and Using Proper Awareness Techniques

John O’Leary, CISSP
Computer Security Institute
Abstract

In trying to educate managers, users and IT personnel on the importance of protecting our information resources, we need to remember that different approaches work for different target audience segments at different ranges of geographical separation. “One size fits all” generally won’t do the job. Top managers need to know things in macro, bottom-line terms. You don’t necessarily have to be there to educate them, but you must be ready to rapidly address their questions. Information security professionals need detailed technical training. Interacting with machines in a lab setting can work very well. Computer users, operators, programmers and IT technicians, webmasters and content developers must be shown what they can do on a day-to-day operational basis. There are just too many of them to cover one-on-one. In this interactive session, we’ll analyze techniques and technologies to ascertain which ones work best in which situations and for which awareness program target groups.
Objectives

At the end of this session, participants will be more able to:

• Ascertain specific information systems security needs for different job functions and environments in their organizations

• Locate areas which need improvement to attain required levels of security compliance

• Identify realistic training options differentiated by content, costs, availability, vendor, and scheduling that will bring weak areas into compliance and prevent solid areas from becoming deficient
Format

• Seminar/Workshop
• Questions at any time
• Anyone can ask
• Anyone can answer

• Sharing of information & techniques
• “Workable” is more important than “elegant”
Agenda

• Defining required security skills
  – The Job
  – The Environment
  – Group Culture
  – Profession Culture
  – Management

• Pinpointing areas of deficiency

• Gaining support

• Delivery methods and techniques

• Locating sources for training and appropriate materials
Required Security Skills
Depend on:

- The job
- The environment
- Group culture
- Profession culture
- Management
The Job

• Working in the Automated Office
  – Includes almost everyone
  – Technophobes to wireheads
  – Some degree of system or network access to get their jobs done
  – Access to information with varying degrees of sensitivity
  – Connectivity, both inside and outside
The Job

- Operating the Systems
  - Multiple people in various positions
    - Classical “operations”
    - LAN administrators
    - Technical support staff
    - Help desk
    - Incident response
    - Communications
    - Security administration / Change control
  - Generally more technical than average user
  - Wider ranging access profiles
The Job

• Developing Products and Processes
  – Webmasters and content developers
  – Development programmers
  – Network architects
  – R&D (not just computer)
  – Technology evaluators
  – Security designers
  – Intranet/Extranet gurus
  – RFID Implementation Group
  – Enterprise I&AM Group
  – Compliance group (??)

• Foster business growth and efficiency
Working in the Automated Office

• Even though people are using the same basic application types:
  – Spreadsheets
  – Word processors
  – Project planners
  – Database engines
  – Messaging networks
  – Search engines
  – Wireless connectivity
  – etc.
Working in the Automated Office

• The **security ramifications** of what they do with these tools and specifically developed products and processes vary widely.

• **That** is what we must focus on when constructing security training plans for our organizations.
Working in the Automated Office

• Generally speaking, the more sensitive and valuable the data that people in a specific job work with, the higher the degree of security required

• Security skills in a visible, critical position must go far beyond the awareness level
Automated Office Workers

• Security skills required for automated office workers will include (but not be limited to):
  – Incident recognition and response
  – Social engineering defense
  – Adhering to compliance mandates
  – Desktop physical security procedures
  – Password discipline
  – Classified item handling
Automated Office Workers

• Security skills required for automated office workers will include (but not be limited to):
  – Privacy protection
  – Criticality recognition
  – Recovery procedures
  – Evidence collection and handling
  – Internet taboos
  – Threat identification
  – . . . . . . . .
The Environment

- Business environmental factors can act to augment security or be detrimental
  - Merger/acquisition/divestiture, even rumors thereof
  - Change at the top – new boss, new direction
  - Labor unrest
  - Outsourcing/offshoring
  - History of recent incidents
  - Industry norms
  - Compliance Activity
  - Regulatory requirements
  - Business Ethics and morals
Group Culture

- Group culture determines “allowable” behavior for members
- Rewards conformity with group norms, whether or not they match organizational policy or sound security principles
- Attempts to change the group culture invariably meet resistance
Group Culture

- Effective training must comprehend the differing group cultures within an organization to strike responsive chords
- Change threatens informal power structures
- Co-opt the informal organization leaders. If they buy in, others will follow
Profession Culture

• Some professions have been notoriously difficult for security practitioners to work with:
  – Physicians
  – Research scientists
  – Engineers
  – Politicians (Internal and External)
  – Customer service reps
  – Computer/network wizards
  – University Professors
Profession Culture

• Tends to be more of an issue in “operators” and “developers” groups (Wizards)
• Any preponderance of specialists
• Security training must be cognizant of the profession’s norms, ethics and ways of doing things:
  – network designers want technical details
  – sales reps want deal-closing leverage points
  – operators want simple, trouble-free backups
Management

- Without their support, there is no security training program
- From a training perspective, they are usually “workers in the automated office”
- Access to extremely sensitive material
- They set the example, whether they want to or not
Management

• To get their support, speak their language
  – Cost/Benefit analysis
  – Expenditures in money, people, resources
  – Payback and effect on mission
  – Response to “Hot Buttons” (Latest virus, HIPAA, S-Ox, GLB, Recovery, Privacy, I&AM, IPS, NAC, database encryption, etc.)

• “Required security skills” will depend on their judgment of how much security is necessary
  – “Handling Sensitive Information” is an area where they’ll usually accept their need for training

• You give input; they make the call
Management

• They’ll need training, too, but it can’t be long and drawn out

• Avoid getting bogged down in technical details, but be prepared to answer their questions in terms of their reality

• They don’t want themselves or the organization to be embarrassed

• Do not patronize them
Pinpointing Areas of Deficiency

• Where inadequate security measures or lack of adherence to security procedures have or can cause significant negative business impact
• Past experiences
• Audit reports
  – internal
  – external
Pinpointing Areas of Deficiency

• Standardized measurements (CSI IPAK)
  – Secure Compass
  – ITIL
  – NIST Publications
  – SAS-70
  – ISO 17799 (now 27001)
  – COBIT
  – COSO
  – ……. 
Pinpointing Areas of Deficiency

- Opinions of:
  - Upper management
  - Area management
  - Area workers (informal org.)
  - Technical people
  - Other security people
  - Consultants (??)
  - Legal
  - Audit group

- Your judgment
# Gaining Support

<table>
<thead>
<tr>
<th>Group</th>
<th>Best Techniques</th>
<th>Best Approach</th>
<th>Expected Results</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Senior Management</strong></td>
<td>Cost justification</td>
<td>Presentation</td>
<td>Funding Support</td>
</tr>
<tr>
<td></td>
<td>Industry comparison</td>
<td>Video</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Audit report</td>
<td>Violation reports</td>
<td></td>
</tr>
<tr>
<td><strong>Middle Management</strong></td>
<td>Demonstrate job performance benefits</td>
<td>Presentation</td>
<td>Support Resource help</td>
</tr>
<tr>
<td></td>
<td>Perform security reviews</td>
<td>Circulate news articles</td>
<td>Adherence</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Video</td>
<td></td>
</tr>
<tr>
<td><strong>Supervision/ Employees</strong></td>
<td>Sign responsibility statements</td>
<td>Presentation</td>
<td>Adherence Support</td>
</tr>
<tr>
<td></td>
<td>Policies and procedures</td>
<td>Newsletters</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Video</td>
<td></td>
</tr>
</tbody>
</table>
Delivery Methods and Techniques

• Briefing
• Formal Presentation
• Lecture
• Workshop
• Seminar
• Case study
• Hands-on Lab
• CBT
Delivery Methods and Techniques

**Presentations**

*PC projector*

*Webinar*

*Flipchart*

*Whiteboard*

*Corporate Security Website*

*No A/V aids*
Delivery Methods and Techniques

**Presentations**

New-Hire Orientations
Department Meeting Presentations
Board of Directors Presentations
Formal Security Courses (e.g. 2-day for new hires)
Delivery Methods and Techniques

• **Section of an existing class**
  
  – Security add-on
  
  – How to use embedded or augmented security features
  
  – Using existing examples
  
  – Make sure not to contradict other class material
  
  – Try not to alter the flow of the class
Delivery Methods and Techniques

• **Videos or DVD’s**
  
  – Home grown
  – Purchased
  – 20 minute maximum
  – Maybe a segment at a time
  – “Brown bag theatre”
  – Someone there to answer questions
Delivery Methods and Techniques

• **Routings of relevant articles**
  – Your organization
  – Competitors
  – Horror stories
  – Recovery sagas
  – **Must be relevant to the receiver**
  – Not too many or too often
Delivery Methods and Techniques

• **Trinkets**
  – with message
  – identity logo
  – at least plausibly usable
    • Ceramic or travel mug
    • coaster
    • squeeze ball
    • wrist rest
    • pen
    • USB hub

  mouse pad
  envelope opener
  wireless signal finder
  candy jar
  paper clip holder
  mini-USB mouse
Delivery Methods and Techniques

• **White papers**
  – “Hot-button” items
  – future technologies
  – context of your organization
  – one-page management summary
  – all the gory technical detail you want after that
Delivery Methods and Techniques

• **Posters**
  – visually appealing
  – visible
  – colorful
  – only one message
  – amusing (?)
  – rotated regularly
  – with a security logo
Delivery Methods and Techniques

Practice

Demos

Practice

Practice

Practice

Practice

Threats
- viruses
- intrusion scenarios
- mistakes/accidents

Countermeasures

to small groups
to large groups
Delivery Methods and Techniques

**Guest speakers**
- Internal
- External Specialists
- Motivators
Delivery Methods and Techniques

**Intranet websites**

- Interesting
- Relevant
- Timely
- Protected
- Pointers to other items
- Contests and prizes
Delivery Methods and Techniques

Intranet Website(s)

Contact information
Names
Phone numbers
Office Location
Pictures
E-mail addresses
Areas of specialization
Backups
Delivery Methods and Techniques

Intranet Website(s)

Policies
Text
Pointers
Interpretation
Examples
Reasoning behind
Draft new policies
Solicitations for comments
Delivery Methods and Techniques

Intranet Website(s)

Procedural Guidelines
FAQ’s
Internal Security Job Postings
Details of Horror and Success Stories
Testimonials
Reader Comments (don’t filter, except for language)
Incident Reporting Forms and instructions
Recovery Plan Information
Audit Emphasis Areas
Publications (Dead Tree)

Security Incident Bulletins & Recaps
“House Organ” articles
Information Protection Tips & Techniques
Internal Security Newsletter
Interpretations of laws/incidents
Publications

Pamphlets/Booklets/Trifolds

Recovery Procedures
Securing Sensitive Information
Things You Should Know & Do when Traveling with a Laptop
Security Reference (What’s where, who to call)
Sarbanes-Oxley and you – A Manager’s Guide
Publications

Security Quarterly Reports

Checklists (e.g., Hacker Incident Response, Possible Virus, Physical Security Incident, Handling Potential Evidence. . . )

Web-based Presentations (e.g., “Getting Connected Securely,” “Our Firewalls,” “Using Anti-virus Software,” . . . . )
Locating Resources and Information

• Internal experiences as sources of learning parables
  – Horror stories
  – Success stories
  – Watch for “airing dirty laundry”
  – Don’t embarrass people

• Yes, these things really can happen here
Locating Resources and Information

• In house expertise:
  – Network designers
  – System wizards
  – Application gurus
  – Virus response team
  – Webmaster
  – Users who have been hit
  – Training experts
  – Other locations of your agency or company
Locating Resources and Information

• External providers:
  – Local SIG’s
  – Security product vendors
  – Other users of the product
  – Web pages
  – Publications
  – Consultants
  – Training firms
Summary

We have covered:

• Defining required security skills
• Pinpointing areas of deficiency
• Training options, including locating sources for training and appropriate materials
The End