U.S. Department of State
Diplomatic Security
The Awareness Team

Lisa Lindholm
Awareness Branch Chief
Office of Computer Security
Bureau of Diplomatic Security
“The secret to enforcement is prevention, and the key to prevention is education.”
R. Wallace Hale
What Is Security Awareness?

- Individual responsibility and sufficient understanding to comply with policies
- Another line of defense
- The best ROI for information security programs
Problems with Awareness Programs

- Not supported by management
- Do not stay current with the infrastructure
- They don’t leverage available delivery mechanisms
- They are not targeted to the appropriate audiences
Awareness Program Lifecycle

- Baseline – Determining the current state
- Develop – Crafting and revising the program
- Deliver – Executing the program
- Measure Progress – Determining and reporting results
Baseline

- Conduct a set of surveys
- Determine level of understanding of key issues, and what to do when faced with them
- Understand threats and vulnerabilities – current and future
- This process helps define scope and requirements of the program
- What are the goals for improvement?
Who – Communities of interest

What – Content, based upon perceived and actual threats and vulnerabilities

How – Delivery channels and frequency
Who and What?

- **Executives** – Return on investment, reduction of risk
- **Information Technology Staff** – Build security into applications, networks, and systems
- **Business Users** – Demonstrate the value of doing business securely
- **New Hires** – Basic fundamentals of a solid security mind-set and the expectations of them with regards to security
What?

- Awareness programs must be agile
  - Policy is less dynamic however, new threats and vulnerabilities appear constantly

- Content must align with policy needs and the realities of threats and vulnerabilities
## Potential Vulnerabilities

<table>
<thead>
<tr>
<th>#</th>
<th>Vulnerability</th>
<th>Easy to Fix?</th>
<th>Perceived Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>E-mail abuse</td>
<td>No</td>
<td>High</td>
</tr>
<tr>
<td>2</td>
<td>Special access privileges and termination</td>
<td>No</td>
<td>High</td>
</tr>
<tr>
<td>3</td>
<td>ID and password sharing</td>
<td>No</td>
<td>High</td>
</tr>
<tr>
<td>4</td>
<td>Malicious code</td>
<td>No</td>
<td>High</td>
</tr>
<tr>
<td>5</td>
<td>Poor password development and misuse (writing passwords down, e.g.)</td>
<td>Yes</td>
<td>High</td>
</tr>
<tr>
<td>6</td>
<td>Employee lack of information security regard, overall</td>
<td>Yes</td>
<td>High</td>
</tr>
<tr>
<td>7</td>
<td>Poor work area (cubicle) security</td>
<td>Yes</td>
<td>Medium</td>
</tr>
<tr>
<td>8</td>
<td>Internet misuse (viewing unauthorized material, e.g.)</td>
<td>Yes</td>
<td>Medium</td>
</tr>
<tr>
<td>9</td>
<td>Software licensing misuse (Software Piracy)</td>
<td>No</td>
<td>Medium</td>
</tr>
<tr>
<td>10</td>
<td>Inappropriate hard-drive storage</td>
<td>Yes</td>
<td>Medium</td>
</tr>
<tr>
<td>11</td>
<td>Corporate espionage, social engineering</td>
<td>No</td>
<td>Medium</td>
</tr>
<tr>
<td>12</td>
<td>Poor workstation security</td>
<td>Yes</td>
<td>Medium</td>
</tr>
<tr>
<td>13</td>
<td>Poor laptop security</td>
<td>Yes</td>
<td>Medium</td>
</tr>
<tr>
<td>14</td>
<td>Misuse of customer or employee personal information</td>
<td>No</td>
<td>Low</td>
</tr>
</tbody>
</table>
Security Awareness Strategies

- Formal or Informal Briefings
- Security education bulletins and department notices
- Security Awareness Month
- Online Computer-based Tutorials
- Newsletters - The Logon
- Security Awareness Posters and Fliers
Summary of “Tried and True” Security Awareness Strategies

- Information Security Websites
  - Policy Guidelines
  - News
  - Frequently Asked Questions
  - Awareness Support E-mail Hotline

- Branded Promotional incentives and Giveaways

- Tip of the Day

- Security Calendars
Summary of “Tried and True”
Security Awareness Strategies

- Learning Management System (LMS)

- Animated Security Awareness DVD’s, CD’s, and online Video vignettes (shorts)

- Executive Briefings

- Eye-catching Security Awareness Posters, Fliers

- Branded Promotional incentives and Giveaways

- Webinars and/or Meetings “In a Box”

- Promotional Art Characters and Themes
Guiding Principles of Message Delivery

- Promote risk management, not security
- Emphasize the benefits
- Engage the audience
- Tell people what they can do to help
- Be dynamic
- Relate practices to employee work
- Encourage questions
Progress Measurement

- Develop metrics that track to improvements of the awareness baseline and with program goals.

- Progress must be measured on two fronts simultaneously:
  - Improvement in security awareness
  - Relative value of content and delivery mechanisms
An important theme is the concept of “ownership” and each community member’s role in achieving program objectives.

A key success factor is the delivery of the right messages to the right people at the right time.

Training should be coordinated centrally, but must be supported deep inside each business unit through the use of training “champions”.
Resources:

- Easyi, Inc.
  www.easyi.com
- Security Awareness Company,
  www.securityawarenesscompany.com
- Techrepublic
  www.rechrepublic
- National Institute of Standards and Technology
  www.itl.nist.com
- The US Agency for International Development (US AID)
  www.usaid.gov
Contacts

- Lisa Lindholm
  Awareness Branch Chief
  Phone: 571-345-2607
  E-mail: LindholmLC@State.gov
Questions?