YEAH, I HAVE A POWERPOINT...

DEVELOPING AN INFORMATION SECURITY AWARENESS PROGRAM

By: Marcia Mangold
DESIRED LEARNING OUTCOMES

- Understand the difference between “Compliance” and “Security” for information awareness training
- Understand the lifecycle of an Information Security Awareness Training program
- Examples of low-cost ideas for awareness training communications, events and activities
Phishing costs corporate America more than 5.9 billion annually.

Workforce members are the greatest source of leaked information.

Social Engineering tactics have surpassed other forms of cyber attacks.

Phishing and social engineering threats are no longer limited to e-mail and include methods such as: Person to Person, SMS messaging (smishing), voice phishing (vishing), and portable media.

More mandates and frameworks require IS Awareness Training...
## WHAT IS AT STAKE...

<table>
<thead>
<tr>
<th>Impact of an attack</th>
<th>Reputational damage</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Time ($$$) lost due to service disruption and remediation</td>
</tr>
<tr>
<td></td>
<td>Loss of intellectual property and sensitive business information</td>
</tr>
<tr>
<td></td>
<td>Potential financial loss</td>
</tr>
<tr>
<td></td>
<td>Affect on National Security</td>
</tr>
</tbody>
</table>

- On average, 30% of phishing emails are opened.
- The #1 delivery vehicle for malware is phishing messages.
- 89% of breaches had a financial or espionage motive.

## COMPLIANCE VS SECURITY

<table>
<thead>
<tr>
<th>Compliance</th>
<th>Information Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>A state of being in accordance with established guidelines, specifications or legislation or the process of becoming so</td>
<td>Measures taken to guard against espionage or sabotage, crime, attack, or loss.</td>
</tr>
<tr>
<td>Doing what is necessary to meet an audit or regulatory compliance.</td>
<td>Doing what is necessary, to reduce risk to an acceptable level.</td>
</tr>
</tbody>
</table>

"being compliant" does NOT guarantee that "something is secure"
WHY AWARENESS TRAINING WORKS

An Information Security training program:

• Addresses your company’s interpretation of applicable security policies, guidelines and regulations
• Supports the business’s activities that mitigate risk
• Measures security based upon the results of baseline assessments, and support IS policies

With Continuous and Varied Security Awareness training, Employees:

• Learn to recognize malicious exploits and how to counteract them
• Are reminded that Information Security Awareness is an every day activity, not just a “training” taken once a year
• Become “Front Line Defenders”, instead of “Hackable Humans”

POWERPOINT VS A TOOL

Traditional Awareness Training

• PowerPoint presentation once a year, supplemented with posters, email alerts, and videos.
• Satisfies compliance

What the experts are saying. What the vendors are trying to sell you

• The vendors try to sell you a “tool” for your information security awareness training.
• A tool only addresses one aspect of your training needs.
• Use vendors as a partner in creating your awareness training program.

What you really need is an Awareness Training Program
INFORMATION SECURITY AWARENESS TRAINING PROGRAM ASSESSMENT

Security Awareness Maturity Model

Where are you? And Where do you want to be?
LIFECYCLE OF AN INFORMATION SECURITY AWARENESS TRAINING PROGRAM

1. Where is your program on the Security Awareness Roadmap
2. Create a charter
3. Make Security Awareness a part of a job description
4. Create metrics and feedback channels
5. Create tactical and strategic and communications plans
6. Update policies and standards to include Security Awareness Training
7. Implement plan
8. Create reports and imports for program
9. Update plan and start over

How do you get there?
## IN THE BEGINNING

**Create a charter**
- Gain buy-in and funding
- Shows that you are serious
- Base program on your internal culture, frameworks, best practices, along with compliance needs

**Make Awareness Training a part of a job description**
- Make it a part of your yearly goals
- Leadership sponsorship
- Training opportunities

**Update policies and standards to include Security Awareness Training**
- Shows everyone else that you are serious
- Lets everyone know what is expected

**Create tactical and strategic, and communications plans**
- Outlines your program and goals to get to the next level
- Gives you a timeline
- Use for budgeting and funding
- Determine who you can partner with inside and outside of the organization
- Determine how you will get your message out
- Determine who needs to know what and when
WHAT’S IN YOUR PROGRAM?

• Partner with other initiatives
• CyberSecurity Month

Events, contests and workshops

• Secure coding training
• Phishing Victims
• Sales & Marketing
• CSRs

Specialized training based on role, job description

• First phish spotter
• Surveys
• Contests

Rewards

• Phishing, vishing, smishing, piggybacking, scams, physical safety, etc.

Emails, articles, videos, testing

• Offer to present at team meetings
• Create Customized training

ATaaS Awareness Training as a Service

• InfraGard, ISSA, ISACA, ISC2, Secureworld

Partnering with other areas inside and outside of the organization

• CBT and Compliance Training
• Sensitive information check (clean desk)

On going Employee assessment program

Remember to “Make it PERSONAL”
## IMPLEMENT REPEATABLE PROCESSES...

<table>
<thead>
<tr>
<th>Rollout Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Set-up</strong></td>
<td>Create environment, create roll-out schedule, develop metrics, and create use cases for pilot</td>
</tr>
<tr>
<td><strong>Pilot</strong></td>
<td>Structured testing of delivery, and actions, using security department resources</td>
</tr>
<tr>
<td>Communications</td>
<td>Communications plan and roll-out of initial information to department heads, helpdesk and selected IT</td>
</tr>
<tr>
<td>Phase</td>
<td>Perform activity</td>
</tr>
<tr>
<td>Retest</td>
<td>Optional activity to determine effectiveness of training.</td>
</tr>
<tr>
<td>Metrics,</td>
<td>Review metrics and combine findings into a report that will be used for awareness training</td>
</tr>
<tr>
<td>reporting, etc.</td>
<td></td>
</tr>
</tbody>
</table>

Since you have to be compliant, start with policy and create “repeatable” processes
REPORTING RESULTS...

Create metrics and feedback channels

• What do you need to know
• What do others need to know
• Use surveys, interviews, etc.

Create reports

• Customize the reports based on the audience
• Think about what needs to be changed, improved or eliminated

The metrics and reports should be based on your goals for the program, actual results that can be supported, and the audience.
BRINGING IN THE CROWD...

- PRIZES OF UNTOLD VALUE!
- SOMETHING THEY CAN USE AT HOME
- SOMETHING THEY CAN SHARE
- SOMETHING THEY WILL REMEMBER

If Possible, make it FUN!
GETTING THE SKILL SETS THAT YOU NEED TO BE SUCCESSFULLY

In-house
- Read articles
- Attend conferences and webinars
- Talk to trainers and teachers
- Take classes
- Hire someone that is part project manager, event planner and IT

Out-source
- Fully to a vendor
- Partnering with a vendor
RESOURCES

FREE

- SANS
  - https://securingthehuman.sans.org/
  - Posters
  - Strategy

- KNOWBe4
  - https://www.knowbe4.com/
  - Scam of the week
  - CyberheistNews

- Dark Reading
  - http://www.darkreading.com/
  - Webinars and News

- SearchSecurity.com
  - http://searchsecurity.techtarget.com/
  - Webinars and News

- YouTube
  - http://youtube.com
  - Videos
  - Ideas

LOW COST IDEAS

- Partnering with other areas, such as communications, physical security, compliance and even facilities

- Ice cream socials, afternoon tea, morning coffee, salsa or chili contest

- Unbreakable password contest

- Caught you doing something right
PUTTING IT ALL TOGETHER

The difference between compliance and security for Information Awareness Training is that your training program should not stop at checking off the boxes.

Create an Information Security Awareness Training Program with a lifecycle.

Explore low-cost ideas for Awareness Training communications, events and activities.

Make it personal.

Remember to have FUN!
Q&A