

Security Awareness & Securing the Human

By: Chandos J. Carrow, CISSP
System Office - Information Security Officer
Virginia Community College System

I am not John Popper nor do I play the harmonica



Question

- Why is October important for Information Security Awareness and Training?
- October is National Cyber Security Awareness Month
- Started 10 years ago
- Sponsored by Department of Homeland Security in cooperation with the National Cyber Security Alliance and the Multi-State Information Sharing and Analysis Center

VCCS and Security Awareness

- 23 colleges and a system office with 40+ locations
- ~15,000 faculty and staff
- Running two programs:
 - MOAT and STH
- 11 colleges and the SO on STH
- ~5,400 seats in STH

Basic Information Security Awareness and Training Program

- Four level approach:
 - Awareness
 - Designed to be presented to all users to focus their attention on security
 - Intended to allow individuals to recognize IT security concerns and respond accordingly
 - Training
 - Strives to produce relevant and needed security skills and competencies
 - Builds upon the information gathered from awareness presentations
 - Education
 - Integrates all of the security skills and competencies of the various functional specialties into a common body of knowledge
 - Strives to produce IT security specialists and professionals capable of vision and proactive response
 - Professional Development
 - Intended to ensure that users possess a required level of knowledge and competence necessary for their roles
 - Validation of skills typically through certification

Where Do Companies Go Wrong

- The Information Security Awareness and Training program was thrown together to meet a requirement
- No planning went into the implementation
- There was no specific budget provided
- Mostly considered an IT Security issue and not very well supported in other departments
- No one is designated as the program administrator or is typically assigned to someone as an additional duty
- Program only consists of an annual presentation that users review and there is nothing throughout the rest of the year to reinforce what they were presented

Awareness VS Training

- In order to have a good Information Security Awareness and Training program you must have a great foundation
- Awareness is that foundation
- An annual presentation is a great start to awareness, but without constant reinforcement that information obtained by users will not set in
- Training should focus more on the specifics of your company and the systems you use, and it does not supersede awareness for any position

Security Awareness Programs and Marketing

- End goal of any security awareness program is to have the end users follow the messages delivered in the program and act in a secure manner
- Awareness programs should not be boring and repetitive
- Marketing focuses on grabbing the attention of the consumer and getting them excited about a product
- Security Awareness Program = Product

STEPPS

- March 2013, Dr. Jonah Berger published a book *Contagious: Why Things Catch On*
- Intrigued by why some videos go viral while some e-mails and posts that seem important do not
- Six principles of contagiousness that helps define whether or not content will go viral
- STEPPS
- Social Currency, Triggers or Cues, Emotion, Public, Practical Value, and Stories

Social Currency

- Resolves around sharing information that makes the individual look smart, contemporary, and up-to-speed on current issues
- In security, social currency can be gained by sharing stories about current cybersecurity news, and then explaining how that news can affect both the company as a whole, individual employees, and their families
- Example: Breach announcements
- Shows how information security affects both their livelihoods and their personal lives

Triggers or Cues

- Can be used to make people think about a product or idea, but within security triggers can be used for following good security practices
- The messages of security awareness should be designed so it is top of everyone's mind
- Example: A nice polo to an employee who wins a security contest may stimulate more focus on following security

Emotion

- Emotional content often gets shared, so focus on feelings
- Ask whether talking about the company's security program generates any emotion or energy
- Craft the messaging so that it brings out some sort of emotion, whether it is laughter or anger
- Example: Send out a story about an elderly lady that is affected by identity theft

Public

- How can you make the action of following the company security program advertise itself?
- Can people see when others are properly following security protocols?
- If not, try to make the security practices more apparent so that they are easier to imitate
- Example: “No piggybacking” and “clean desk” policies can be implemented and those “good practitioners” can be publicly rewarded

Practical Value

- People are more likely to utilize the content of a message if it has some practical value for their lives
- How does complying with corporate security help people to help others and themselves?
- How can the security awareness program be configured so that others want to talk about it and the good practices within?
- Give your users the “carrot” rather than the “stick”, emphasize the benefits of security rather than the penalties.

Stories

- How can a security program expand so that it is “advertised” through stories and viral means that people want to share?
- Use stories to share lesson learned or morals, but make it interesting not boring police blotter narratives
- Instead, build in characters and fun elements that make the employees want to tell the stories again at work and at home

Creating/Redesigning an Information Security Awareness and Training Program

- Many companies already have a program, but the steps for creating a new program can be used to redesign your current program as well
 1. Ensure you have upper management support
 - a. Resources
 - b. Commitment
 2. Create an Information Security Awareness and Training program team
 - a. Most influential members of each department
 - b. Members should be dedicated to the cause and will be active participants
 - c. Do not have to be technically/security savvy to be part of the team
 - d. If team members are not active, they are reported to management and a replacement requested

3. Define the roles and responsibilities that each person/department will play within this program
 - a. Create policies, standards, guidelines, and procedures
4. Determine what type of program management model you will use for your company
 - a. Centralized, Partially Decentralized, or Fully Decentralized
5. Conduct a Needs Assessment
 - a. Complete interviews, surveys, review resource material, etc.
6. Have a clear mission and directives

7. Listen and analyze the user feedback
8. Determine where are the gaps between what is currently being done and what is required
9. Explore your options for deploying your program
 - a. Company generated material, third-party generated material hosted on internal Learning Management System (LMS), or third-party hosted solution
10. Develop the strategy and plan of the program
 - a. Current regulations, scope, goals, target audience, learning objectives, topics, mandatory/optional courses, evidence of learning, frequency

11. Implementation Schedule

- a. Establish your priorities especially if this implementation is to be done in a phased approach
 - 1. Availability of material/resources
 - 2. Role and organizational impact
 - 3. State of current compliance
 - 4. Critical project dependencies

12. Setting the bar

- a. Determine the complexity of the material presented based on the target audience

13. Funding the program

- a. Percent of overall training budget
- b. Allocation per user by role
- c. Percent of overall IT budget
- d. Explicit dollar allocation by component based on overall implementation costs

Delivering Awareness Materials

- Messages on awareness tools
 - Pens, key fobs, notepads, bookmarks, etc.
- Posters
- Screensavers
- Popup messages when people log into their computers
- Newsletters
- Company wide e-mail messages

- Videotapes (YouTube videos)
- Web-based sessions
- IT security days
- Changing the IT security webpage
 - Current awareness theme
 - Helpful information and tips
- “Brown bag” seminars
- Mascots
- Crossword puzzles and other games
- Award program
- Do and Don’t list
- In-person instructor-led sessions

Keeping Your Program Up-to-date

- A program is never complete
 - Always listen for and read about new threats
 - Policies and standards do change
- Always be open for feedback from users
 - The program is designed for them
 - If they do not like it then they will not take it seriously
- On at least a semi-annual basis the team should review the materials and presentations of the program
 - If materials/presentations come from a third-party then they should have some review/update process

- Surveys
- Benchmarking
- Technology Shifts
- Focus Groups
- Interviews
- Status Reports
- Independent Observations
- Evaluation Forms

Success Indicators

- Sufficient funding to implement the agreed-upon strategy
- Appropriate organization placement to enable those with key responsibilities to effectively implement the strategy
- Support for broad distribution and posting of security awareness items
- Executive/senior level messages to staff regarding security
- Use of metrics
 - Decline in security incidents or violations, gap between existing awareness and training coverage and identified needs is shrinking, etc.
- Managers do not use their status in the organization to avoid security controls
- Increase in the level of attendance at mandatory security forums/briefings
- Recognition of security contributions
- Motivation is demonstrated by those playing key roles in managing/coordinating the security program

Helpful Tips

- Keep your awareness material interesting and up-to-date
- Repeating an awareness message and using different ways to present that information will increase the retention by the users
- Make sure that the delivery of the awareness material is easy to use and understand, is scalable, and does not impact the work production of the users
- Deliver updates on a monthly/quarterly basis to your Senior Leadership and/or Board of Directors
- After implementation of the program, continue having at least monthly meetings of your team because a program is never finished it should be continually modified to meet the needs of your company and addresses the new threats on cyber security

Resources

- <http://infosecresources.com/security-awareness.html>

Information Security Resources

Information Security

Monday September 30, 2013

[About the Founder](#)

[Contact](#)

[Mailing List](#)

[RSS Feed](#)

[Awareness Program](#)

[INFOSEC Professional](#)

[INFOSEC Program](#)

[INFOSEC Auditing](#)

[Risk Management](#)

[Insider Threat](#)

[Application Security](#)

[Incident Response](#)

[Reports & Stats](#)

[Home Page](#)



SECURITY AWARENESS PROGRAMS

[NIST 800-50: Security Awareness and Training Program](#)

This NIST publication provides detailed guidance on designing, developing, implementing, and maintaining an awareness and training program within an agency's IT security program.

[ENISA: A Users' Guide: How to Raise Information Security Awareness](#)

This document illustrates the main processes necessary to plan, organise and run information security awareness raising initiatives: plan & assess, execute & manage, evaluate & adjust. Each process is analysed and time-related actions and dependencies are identified. The process modelling presented provides a basis for "kick-starting" the scoping and planning activities as well as the execution and assessment of any programme. The Guide aims to deliver a consistent and robust understanding of major processes and activities among users.

[NIST 800-16: Information Technology Security Training Requirements \(188 pages\)](#)

The overall goal for use of this document is to facilitate the development or strengthening of a comprehensive, measurable, cost-effective IT security program which supports the missions of the organization and is administered as an integral element of sound IT management and planning. Protecting the value of an organization's information assets demands no less. This approach allows senior officials to understand where, in what way, and to what extent IT-related job responsibilities include IT security responsibilities, permitting the most cost-effective allocation of limited IT security training resources.

[Appendix A-D](#) [Appendix E](#)

[Building a Security Awareness Program - CyberGuard](#)

Hackers, worms and viruses grab the headlines, but the real threat often comes not from outside the organization but within. Social engineering and unhappy employees pose very real risks to network security. How do you address the problem? This article offers a practical approach to setting up an effective security awareness program that gets everyone in the organization on board.

[Security Awareness Toolbox - The Information Warfare Site](#)

The Security Awareness Toolbox contains many useful documents and links. The Main Documents section was contributed by Melissa Guenther. The Toolbox is a rich source of awareness material.

[SANS Reading Room - Security Awareness Section](#)

Most of the computer security white papers in the Reading Room have been written by students seeking GIAC certification to fulfill part of their certification requirements and are provided by SANS as a resource to benefit the security community at large.

[University of Arizona Security Awareness Page](#)

The UA security awareness site contains awareness presentations, videos and posters. It's a good site to explore.

[IIA Tone at the Top Awareness Newsletter](#)

Mission: To provide executive management, boards of directors, and audit committees with concise, leading-edge information on such issues as risk, internal control, governance, ethics, and the changing role of internal auditing; and guidance relative to their roles in, and responsibilities for the internal audit process.

Security Awareness Tips

[Stop.Think.Connect.](#)

The Stop.Think.Connect. Campaign is a national public awareness campaign aimed at increasing the understanding of cyber

INFOSEC List:

[The Insider Threat](#)

[Software Development: Building Security In](#)

[Application Security](#)

[Protect Internal Networks from Internet Exposure](#)

[Support for Strong Authentication](#)

[Top](#)

[Home](#)

[Contact](#)

Questions



Thank You

Contact info:

Chandos Carrow

ccarrow@vccs.edu