Security Awareness Roadmap

Just like computers, people store, process, and transfer information. However, very little has been done to secure this "human" operating system, or HumanOS. As a result, people rather than technology are now the primary attack vector. Security awareness training is one of the most effective ways to address this problem. This roadmap is designed to help your organization build, maintain and measure a high-impact security awareness program that reduces risk by changing people’s behavior and also meets your legal, compliance, and audit requirements. To use this roadmap, first identify the maturity level of your security awareness program and where you want to take it. Then follow the detailed steps to get there.

No Awareness Program

Program does not exist. Employees have no idea that they are a target, do not know or understand organizational security policies, and easily fall victim to cyber or human-based attacks.

How To Get There:
- Identify compliance of audit standards that your organization must adhere to.
- Identify awareness requirements for those standards which will likely require coordination with compliance or audit offices.
- Develop or purchase training to meet those requirements.
- Deploy security awareness training.
- Track who completes training.

Deliverables:
- Annual training materials such as videos, newsletters and online presentations.
- Reports of who has and who has not completed required training.

Standards Requiring Awareness Training
- ISO/IEC 27002:2012 2.2
- PCI DSS §12.6
- SOX §404(a) (1)(c)
- GLBA §6801(b)(1)(3)
- NIST SP 800-50
- ISO/IEC 27002 §8.2.2
- NERC §CIP-004-3(B)(R1)
- GLBA §6801.(b).(1).(3)
- SOX §404(a).(a).(1)
- PCI DSS §12.6
- ISO/IEC 27002 §8.2.2

Compliance Focused

Program designed primarily to meet specific compliance or audit requirements. Training is limited to annual or bi-annual basis. Employees are unsure of organizational policies, their role in protecting their organization’s information assets, and how to prevent, identify, or report a security incident.

How To Get There:
- Identify compliance of audit standards that your organization must adhere to.
- Identify awareness requirements for those standards which will likely require coordination with compliance or audit offices.
- Develop or purchase training to meet those requirements.
- Deploy security awareness training.
- Track who completes training, and when.

Deliverables:
- Annual training materials such as videos, newsletters and online presentations.
- Reports of who has and who has not completed required training.

Standards Requiring Awareness Training
- ISO/IEC 27002:2012 2.2
- PCI DSS §12.6
- SOX §404(a) (1)(c)
- GLBA §6801(b)(1)(3)
- FISMA §5(a)(4)-§5(a)(18)
- HIPAA §16.3.3(a)
- NERC §C2-004-3(R1)
- NIST SP 800-50

Promotes Awareness & Change

Program identifies the training topics that have the greatest impact in supporting the organization’s mission and focuses on those key topics. Program goes beyond just annual training and includes continual reinforcement throughout the year. Content is communicated in an engaging and positive manner that encourages behavior change at work, home, and while traveling. As a result, employees, contractors and staff understand and follow organizational policies and actively recognize, prevent and report incidents.

How To Get There:
- Begin by identifying stakeholders in your organization. Those are the individuals who are key to making your program a success. Once identified, build and execute a plan to gain their support. Methods to gain support include a human risk survey or phishing assessment. For additional examples refer to the Metrics section.
- Create a Project Charter that gives you authorization to begin the planning process. The Project Charter should set key expectations including identifying the project manager, project scope, project goals, milestones, and assumptions.
- The management reviews the Project Charter. Once it is approved planning can officially begin.
- Establish a Steering Committee to assist in planning, executing, and maintaining the awareness program. Steering Committee should include 5-10 volunteer advisors from different departments or business units within your organization.
- Identify WHO you will be targeting in your program. Different roles may require different or additional training, including employees, help desk, IT staff, developers, and senior leadership.
- Identify WHAT you will communicate to the different groups targeted by your program. The goal is to create the shortest training possible that has the greatest impact. Begin with a risk analysis to identify the different human-based risks to your organization, document those risks in a matrix, and then prioritize the risks from high to low. Select which tasks you will address in your program based on priority level, like restrictions and other organizational requirements. Create a separate Learning Objectives document for each topic that identifies the specific behavior you need to change.
- Once you have determined WHO and WHAT is part of your awareness program and WHAT you will teach them, determine HOW you will communicate that content. To create an engaging program focus on how people will benefit from the training, how it meets their daily tasks, and how personal this is for them. There are two categories of training: Primary and Reinforcement. Primary training teaches new content and is usually taught annually or more often. Reinforcement training is an ongoing commitment throughout the year to reinforce key topics. Common examples of reinforcement training include newsletters, posters, podcasts, assessments and blog. When teaching a specific topic, refer to that topic’s Learning Objectives document to determine what content to communicate. This may require the different way you communicate a topic, the message will always be consistent.
- Create an execution plan in coordination with your Steering Committee. The plan should begin with WHY you are launching a security awareness program and its goals and overall scope. Then document WHO you will target in your awareness program, WHAT you will teach them and HOW, include a timeline that identifies key milestones and the launch date of this program, organizational involvement and any other relevant information. Your organization’s risk may require for planning purposes.
- Have management review the plan. Once the plan is approved you can execute your awareness program. Make sure that senior stakeholder (such as your CEO) communicates the importance of the entire program, both behavioral training and other information that may be required for planning purposes.

Deliverables:
- Stakeholder matrix
- Gaining stakeholder support presentation
- Human risk survey
- Project Charter

Steering Committee matrix
Topic matrix
Learning objectives document for each topic
Execution plan

About the Poster

This roadmap was developed as a consensus project by security professionals actively involved in security awareness programs. If you have any suggestions or would like to get involved please contact community@securingthehuman.org

Contributors Include:
- Randy Marchay (McAfee), Connelly, Stephany (Cigna), Ake Solis (Wounded D0g)
- Todd Dudley (Honeyway), John Andrew (Honeyway), Peter Danheux (BAE Systems, Patuxent River), Colleen O’Connor, Christopher Isern (State of Nevada), Jenifer L. Boulanger (NIK-Mark), Mark Moskowitz (Way2), B. Scott Bigrigg (Texas Tech University), Tracy Gunter (Arizona State University), George Bautista (Risk Intelligence), Greg Aufrichtig (Fbi, Salt Lake)
- Janet Roberts (Progressive Insurance), Chris Storms (CSSC), Capital)
- Mary Naphon (Lincoln Financial Group), Dave Vaughan (HP, Enterprise Services), Tim Harwood (Bt), Tina Craig (Bt), Dan Heilbronn (CA), Eric Peloso (Us State National Bank), Antonia Merola

5 Long-Term Sustainment

Program has processes and resources in place for a long-term life cycle, including at a minimum an annual review and updates of both training content and communication methods. As a result, the program is an established part of the organization’s culture and is current.

How To Get There:
- Identify what you will review your awareness program annually.
- Identify new or changing technologies, threats, business requirements, or compliance standards that should be included in your annual update.
- Conduct an assessment of your organization’s security awareness level and compare that to the baseline taken in step 3.
- Survey staff to feedback including what elements are most important about the program, what needs to be changed, which topics are most interesting, and which behaviors they are adopting.
- Review all the topics you are communicating and identify if new topics need to be added, and which existing topics should be removed or updated.
- Once topic changes have been identified, review and update the learning objectives for each topic.
- Review how the topics are communicated, which methods have had the greatest impact, and which need to be updated or dropped.
- Conduct an annual review and update of the budget to align with changing business objectives.

Deliverables:
- Metrics matrix
- Examples of Metrics:
  - No. of people who fall victim to phishing attacks
  - No. of successful attempts
  - No. of breaches
  - No. of security audits
  - No. of policy changes
  - No. of employees trained
  - Employee access to framework
  - % of users sampled with positive attitude towards a framework
  - % of users sampled who believe their actions can have an impact security

Additional Materials:
- NIST SP800-50 Building an Information Security Awareness Program
- How to Raise Information Security Awareness
- IT Controls
- Top Critical Controls
- Twenty Critical Security Controls for Effective Cyber Defense

Documents followed by this icon may be downloaded at: www.securingshethuman.org/resources/planning