



# 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.

## 1 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 attacks or their own mistakes.

### 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](mailto:community@securingthehuman.org)

**Contributors Include:** Randy Marchany (Virginia Tech), Cortney Stephens (Union Gas), Julie Sobel (Alliance Data), Tonia Dudley (Charles Schwab), John Andrew (Honeywell), Pieter Danhieux (BAE Systems Detica), Vivian Gernand (Corning), Christopher Ipsen (State of Nevada), Jenn Lesser (Facebook), Mark Merkow (PayPal), Sam Segran (Texas Tech University), Tracy Grunig (Arizona State University), Geordie Stewart (Risk Intelligence), Greg Aurigemma (Flight Safety), Janet Roberts (Zurich Insurance), Chris Sorensen (GE Capital), Mary Napphen (Lincoln Financial Group), David Vaughn (HP Enterprise Services), Tim Harwood (BP), Tanja Craig (BP), Dave Piscitello (ICANN), Eric Phifer (Seacost National Bank), Antonio Merola.

## 2 Compliance Focused

Program designed primarily to meet specific compliance or audit requirements. Training is limited to annual or ad-hoc 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 or audit standards that your organization must adhere to. ⬇
- Identify security awareness requirements for those standards, which will likely require coordination with compliance or audit officer.
- 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 on-site presentations. ⬇
- Reports of who has and who has not completed required training.

### Standards Requiring Awareness Training

- ISO/IEC 27002 §8.2.2
- PCI DSS §12.6
- SOX §404(a).(a).(1)
- GLBA §6801.(b).(1).(3)
- FISMA §3544.(b).(4).(A).(B)
- HIPAA §164.308.(a).(5).(i)
- CIP-004-5.1 R1
- EU Data Protection Directive

## 3 Promoting Awareness & Behavior 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. These 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, awareness assessments, root cause analysis of recent incidents, industry reports, or cost-benefit analysis.
- Create a baseline of your organization's security awareness level, such as with 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, cost estimates, program scope, goals, milestones, and assumptions. Have management review 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. New awareness programs tend to start with a single target group, all employees, while more mature programs add additional target groups that require additional or more specialized training.
- 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. Then select which risks you will address in your program by priority. These risks determine the topics you will teach. Then create a separate Learning Objectives document for each topic and identify the key behaviors you need to change to manage those risks.
- Once you have determined WHO is the target 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 most of the lessons apply to their personal lives. There are two categories of training: Primary and Reinforcement. Primary training teaches new content and is usually taught annually or semi-annually and either on-site or online. Reinforcement training is employed throughout the rest of the year to reinforce key topics. Common examples of reinforcement training include newsletters, posters, podcasts, assessments, and blogs. When teaching a specific topic, refer to that topic's Learning Objectives document to determine what content to communicate. This way, regardless of the different ways 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 the program, critical resources involved, and any other relevant information your organization may require for planning purposes.
- Have management review the plan. Once the plan is approved, you can execute your awareness program. Have the most senior stakeholder (such as your CEO) announce the program to the organization, such as by email, blog posting, or taped video.

### Deliverables:

- Stakeholder and Steering Committee matrices ⬇
- Human risk survey ⬇
- Project Charter ⬇
- Topics matrix ⬇
- Learning objectives document for each topic ⬇
- Execution plan ⬇

## 4 Long-Term Sustainment

Program has processes and resources in place for a long-term life cycle, including (at a minimum) an annual review and update of both training content and communication methods. As a result, the program goes beyond just changing behaviors and begins to change the culture of the organization.

### How to Get There:

- Identify when you will review your awareness program each year.
- 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 stage 3.
- Survey staff for feedback, including what elements they liked best about the program, what needs to be changed, which topic they found most interesting, and which behaviors they changed.
- Conduct a human risk analysis and compliance review to determine if there are any new topics that need to be added or updated in your program.
- 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 methods need to be updated or dropped.
- Conduct an annual review and update of the budget to address changing business objectives.

### Deliverables:

- Content tracking matrix used to document which topics and learning objectives were updated, by whom, and when. ⬇

## 5 Metrics Framework

Program has a robust metrics framework to track progress and measure impact. As a result, the program is continuously improving and able to demonstrate return on investment.

### How to Get There:

- There are two categories of metrics for security awareness programs: Compliance and Impact. Compliance metrics measure the compliance of your program. They are used by auditors to ensure your program is compliant with specific regulations and standards. Impact metrics measure the impact your awareness program is having, specifically, what behaviors have you changed and the impact that has to your organization.
- Identify key human risks you are attempting to manage, then identify metrics that best measure those risks.
- Document how and when you intend to measure the metrics.
- Identify who to communicate results to, when, and how.
- Execute metrics measurement.

### Deliverables:

- Metrics matrix. ⬇

### Compliance Metrics:

- Number of people who have completed the training.
- Number of employees who have signed the Acceptable Use Policy.
- Number of newsletters or posters distributed.
- Number of on-site training sessions.

### Impact Metrics:

- # of employees who fall victim to phishing simulations.
- # of sensitive documents in dumpster.
- # of mobile devices with a passcode.
- # of infected systems each month.
- % of people sampled with positive attitude towards information security.
- % of people who believe their coworkers have shared passwords with others.



[securingthehuman.sans.org/planning](https://securingthehuman.sans.org/planning)