A Heightened Sense of Awareness

What the Internal Auditor Should Know About Information Security Awareness Training

According to the US National Institute of Standards and Technology (NIST), each individual in an organization who owns, uses, relies on, or manages information and information systems must fully understand his or her specific security responsibilities.[1]

One of the most important tools an organization has (or should have) to reach that state of readiness is an information security awareness training program.

Even though internal auditors may not be performing an audit of the security awareness training program specifically, they should be familiar with the elements of a good awareness program regardless of the business area at which they are looking. If there are issues in a security-related area, awareness training may be one place they can look to provide recommendations.

The key characteristics of an information security awareness training program that an internal auditor should be aware of include the extent to which the program is supported by management, the content of the training itself, how that training is delivered and how the organization measures success for the program.

Management Support

A successful information security awareness training program must have the support of senior management for the obvious reason that it requires the commitment of resources (money and employee hours). Beyond that, senior management must see to it that:

- The program content and delivery are well suited to the needs of the organization.
- The training is understood and retained well enough to influence employee behavior.
- The organization receives value from the program in terms of mitigating security risk.

Finally, and perhaps most important, senior management should reinforce the awareness training by setting a good top-down example in their behaviors and attitudes. “The critical success factor [for an information security awareness program] is

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

https://bit.ly/2Pbw1DP

Wade Cassels, CISA, CFE, CIA, CRMA
Is a senior IT auditor at Nielsen. He supports Nielsen’s IT general controls external audit engagement and the audit reporting and communications functions for Nielsen Internal Audit.

Kevin Alvero, CFE
Is senior vice president of internal audit at Nielsen. He leads Nielsen’s global internal quality audit program and its industry standards compliance initiatives, spanning the company’s television, digital, and consumer products and services.

Randy Pierson, CISA
Is a senior IT auditor at Nielsen and has worked in the media and entertainment industry since 2011. Before joining Nielsen, he worked as an auditor with Ernst & Young, where he served organizations across the media industry, including television, Internet and mobile audience research. Pierson also served as compliance officer for the digital media company Pixalate.

IN THE CAT-AND-MOUSE GAME OF PROTECTING ORGANIZATIONAL ASSETS, SECURITY THREATS ARE CONSTANTLY EVOLVING, SO SECURITY AWARENESS TRAINING IS NEVER DONE.

how well top management acts as role models for its employees," writes V. J. Srinvas in a recent ISACA Now blog post. "Their actions will influence and enhance policy compliance and awareness levels among employees."[2]

Content

The most important aspect of good security awareness training content is making sure it is customized to the audience based on their job area, role and user level. It would not be productive, in fact, it would be counterproductive, to teach general staff about security threats and policies/processes that are specific to technical users, such as programmers or personnel who maintain system architecture. In addition to the obvious benefit of aiding retention, keeping training at an appropriate technical level also helps to ensure that knowledge of more complex and technical security processes is limited in its exposure to those who need to know. However, it is important to provide all trainees enough visibility to understand how their everyday roles fit into the big picture of the organization's overall security risk management. All users should understand, for example, not just that they are required to update their password(s) regularly, but they should also be able to articulate how password protocols help protect them and the organization.

Even though security awareness training is often provided by a third-party vendor, it is important that multiple areas of the organization contribute to the development of the training content to ensure that the content is well suited to the organization's needs and the risk environment in which it operates. Input related to content should not only come from places such as security, IT, information security and legal, but also from operational leaders who can provide insight into how general users interact with security risk/threats in the course of their day-to-day duties so that the training provider (whether internal or third party) can cater to that risk. The internal auditor should also be aware if his or her organization is practicing sound vendor risk management practices. As one author noted, "Companies must perform [due diligence] on any organization they consider to provide outsourced online training to employees."[3]

From a content perspective, good training should consist of real-world examples that are relatable to the trainees' everyday work. It should also include real-world case studies that help to reinforce the reality that security breaches do happen and demonstrate how the organization can be impacted.

Finally, awareness training must be compliant with any relevant standards or regulations (such as the US Federal Information Security Management Act [FISMA]), based on the organization's geography, industry type, etc.

Format/Delivery

In the cat-and-mouse game of protecting organizational assets, security threats are constantly evolving, so security awareness training is never done. It should be performed on a routine basis and updated regularly. Generally, trainees are better able to understand and retain smaller amounts of information presented in regular increments.

The training should also come from a variety of different delivery methods. An article published by the SANS Institute says,

> *One of the best ways to make sure company employees will not make costly errors in regard to information security is to institute company-wide security-awareness training initiatives that include, but are not limited to classroom style training sessions, security awareness website(s), helpful hints via e-mail, or even posters. These methods can help ensure employees have a solid understanding of company security policy, procedure and best practices.*[4]

In-person classroom training, which may be the most resource intensive and, therefore, the least frequent, can be complemented by more frequent online training (modules or live virtual sessions) and by even more frequent email or newsletter communications. Using these different types of delivery methods in concert allows organizations to control costs, disseminate information with agility and achieve understanding by different types of learners. Incorporating user communities also gives employees access to support for questions or issues as they arise.

Regardless of the delivery type, there should be some interactive element to the training. Interactivity helps to ensure participation and promote retention. Online modules may have pop-up quizzes or other checks for understanding, for example. In live classroom or live virtual training, attendees should have the opportunity to ask questions.

Measurement

A good security awareness program must have metrics that help management make informed judgments about its effectiveness. Generally, these metrics fall into three main categories:

- **Participation**—Are the right people receiving the training when needed? This is the easiest part of the program to measure and, although participation alone is not sufficient to judge success, it is, nevertheless, important to track.
- **Retention**—Are trainees understanding the material that is being taught? Not only is this important to capture on a session-by-session basis, but tracking this information over time will help management and vendors make incremental improvements to the content and structure of the awareness training program.
- **Compliance**—Are employees carrying the knowledge forward into their roles? There are a number of ways organizations can measure if awareness training is affecting employee behavior, including incident tracking and review, penetration testing (i.e., hacking, phishing, social engineering), and internal audits of adherence to policies such as data retention, password and off-boarding protocols.

However, using these measurements to make an assessment about the value of the training program to the organization—its return on investment (ROI)—can be one of the more challenging aspects of managing the program. For the internal auditor, who is conditioned to think of risk in terms of likelihood and impact, it is helpful to consider whether the training program is mitigating either, or both. For example, if having an awareness program is a matter of compliance, then avoiding the costs of noncompliance (i.e., fines, reputational damage) obviously contributes to ROI. Meanwhile, if the estimated financial impact of an event (e.g., a particular information security breach) is known based on the organization's risk assessment process, then a change in the organization's level of susceptibility (i.e., likelihood), which can be measured, can provide management with an idea of the return they are getting from awareness training.

The key is having the measurements in place on which to base ROI calculations prior to implementing the training. As one expert notes, "If you have a concrete (or at least evidence-based) way to track susceptibility, measuring ROI is simple."[5]

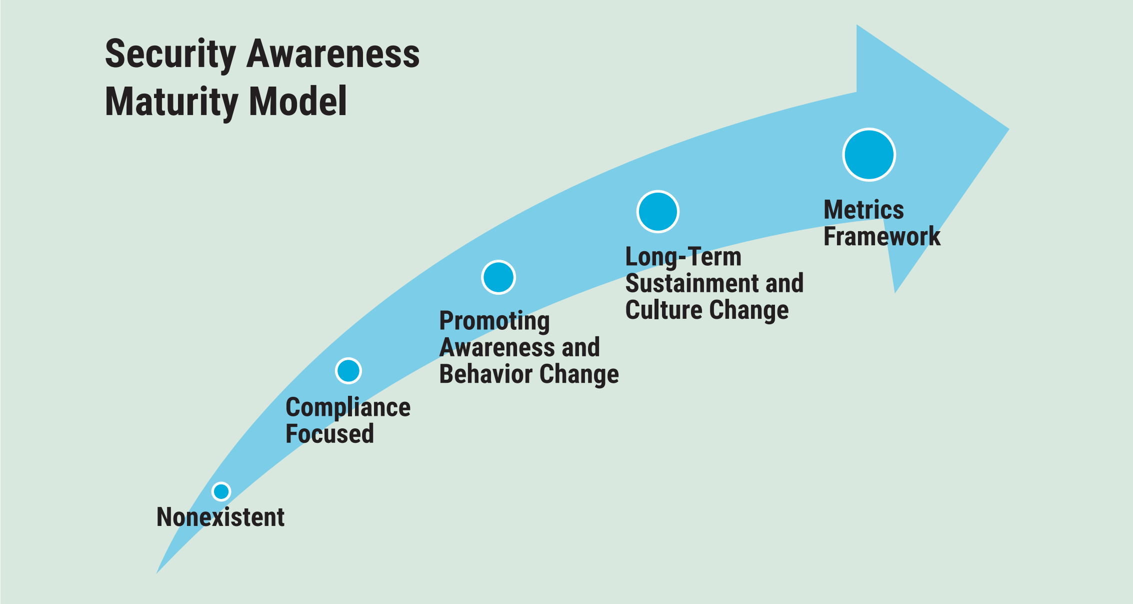
> "A GOOD SECURITY AWARENESS PROGRAM MUST HAVE METRICS THAT HELP MANAGEMENT MAKE INFORMED JUDGMENTS ABOUT ITS EFFECTIVENESS."

Maturity

In 2016, SANS introduced the Security Awareness Maturity Model (**figure1**). The internal auditor should understand where on the spectrum his or her organization falls, but, perhaps more important, the internal auditor should determine whether or not a maturity model is being utilized by management to guide the content, frequency, delivery and measurement of the security awareness training program over time. Per the SANS website,[6] the spectrum of maturity levels are defined as follows:

- **Nonexistent**—Program does not exist. Employees have no idea that they are a target, that their actions have a direct impact on the security of the organization, do not know or understand organization policies, and easily fall victim to attacks.

Figure 1—Security Awareness Maturity Model


Security Awareness Maturity Model
Metrics Framework
Long-Term Sustainment and Culture Change
Promoting Awareness and Behavior Change
Compliance Focused
Nonexistent

Source: SANS, "Defining the Security Awareness Maturity Model," Security Awareness blog, 8 March 2016, *https://www.sans.org/security-awareness-training/blog/defining-security-awareness-maturity-model.* Reprinted with permission.

- **Compliance focused**—Program is designed primarily to meet specific compliance or audit requirements. Training is limited to annual or *ad hoc* basis. Employees are unsure of organizational policies and/or their role in protecting their organization's information assets.
- **Promoting awareness and 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, people understand and follow organization policies and actively recognize, prevent and report incidents. Behavior can begin to be changed in as early as several weeks, depending on the behavior being targeted.
- **Long-term sustainment and culture change**—Program has the processes, resources and leadership support in place for a long-term life cycle, including, at a minimum, an annual review and update of the program. As a result, the program is an established part of the organization's culture and is current and engaging. It takes a minimum of 3-5 years to effectively change culture.
- **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. This stage does not imply metrics are not part of every stage (they are). This stage reinforces that to truly have a mature program, it must have metrics to demonstrate success.

Conclusion

For an organization's employees to react appropriately to the security threats they encounter and to avoid unknowingly becoming a security threat themselves, they must receive regular, relevant and engaging information security awareness training. That is why the internal auditor should be able to recognize and articulate the elements (or missing elements, as the case may be) of an effective security awareness training program that delivers value to the organization.

Endnotes

1 Klein, P. ; P. Toth; *A Role-Based Model for Federal Information Technology/Cybersecurity Training*, 2013, *https://csrc.nist.gov/csrc/media/publications/sp/800-16/rev-1/draft/documents/draft_sp800_16_rev1_2nd-draft.pdf*

2 Srinivas, V. J.; "How to Make Information Security Awareness Relevant," ISACA Now blog, *www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?ID=711*

3 Kroll, K.; "Kicking the Tires on Third-Party Online Training Offerings," *Compliance Week*, 9 September, 2014, *https://www.complianceweek.com/news/news-article/kicking-the-tires-on-third-party-online-training-offerings#.WyQGkjQvzIU*

4 Brodie, C.; *The Importance of Security Awareness Training*, SANS, 2008, *https://www.sans.org/reading-room/whitepapers/awareness/importance-security-awareness-training-33013*

5 Dowd, J.; "How to Calculate ROI for Security Awareness Training," The PhishLabs Blog, 22 November 2016, *https://info.phishlabs.com/blog/how-to-calculate-roi-for-security-awareness-training*

6 SANS, "Defining the Security Awareness Maturity Model," 8 March 2016, *https://www.sans.org/security-awareness-training/blog/defining-security-awareness-maturity-model*