Keywords: cybersecurity, compliance, security awareness, training

Cybertrust

Security Awareness Training for the Workforce: Moving Beyond "Check-the-box" Compliance

Julie Haney, National Institute of Standards and Technology

Wayne Lutters, University of Maryland

Security awareness training requirements set a minimum baseline for introducing security practices to an organization's workforce. But is simple compliance enough to result in behavior change?

Given the high stakes and rapidly changing threat landscape of cybersecurity today, orienting an entire organization towards security practices is an important, but non-trivial, undertaking. A starting point is security awareness training, which is twofold – awareness seeks to change organizational attitudes while training gives employees the skills and tools to practice good security hygiene[1].

It is common for various public and private industry sectors to mandate security awareness training for their workforce. For example, within the U.S., the Gramm-Leach-Bliley Act for the financial sector and the Federal Information Security Modernization Act of 2014 for federal agencies mandate security awareness training. The European Union's General Data Protection Regulation requires organizations to provide similar training. A good example from the private sector is the Payment Card Industry (PCI) Security Standards Council, which makes awareness training available to people who must comply with the PCI Data Security Standard.

These mandates, policies, and standards establish a measurable, minimum baseline. The hope is that compliance with these training requirements will result in long-term positive impacts on security behaviors, such as securely handling cardholders' data in the case of PCI, thus improving the overall security posture of organizations. But does compliance-based training live up to its promise?

When Compliance Is Not Enough

Despite its noble intent, security awareness training can develop a bad reputation within an organization, sometimes with good reason. Training may be stereotypically boring – "death by PowerPoint" presentations and their corresponding computer-based quizzes – with the same generic content year after year. Furthermore, this annual refresh is likely susceptible to diminishing learning effects when not regularly reinforced with practice.

In addition to the lackluster way in which training is presented, those tasked with managing it may be at a disadvantage. Often plucked straight from the ranks of a firm's security professionals with little understanding of "people issues," they may be given insufficient guidance or resources to perform these additional duties[2].

Most importantly, the training's impact may never really be fully known. Some organizations view training simply as a "check-the-box" exercise, measuring success solely by training completion rates. However, this reveals little about how effective the training is in changing and sustaining attitudes and behaviors.

Taking It to the Next Level

Although security awareness training may get a bad rap, this type of compliance activity can be beneficial as it ensures the workforce is at least exposed to security concepts and practices. But, recognizing that training compliance just sets a minimum bar, what are the next, evolutionary steps?

We suggest that the goal of security awareness training should never just be to "check the box," but rather to move employees toward intrinsic motivation where they see the value of security, develop curiosity to learn more on their own, feel a sense of ownership and empowerment, want to the do the right thing, and as a result actually practice good behaviors. If resources allow, consider bringing in an outside consulting firm with expertise in security awareness training to help your program progress and measure success. Otherwise, there is plenty your own security awareness team can do. Based on best practices gleaned from seasoned security awareness professionals and our prior research studying security advocacy and awareness[3], we offer the following suggestions to prompt organizations to rethink existing security awareness training and take their programs to the next level.

Become an Advocate

Instead of viewing the security awareness team as merely compliance managers, consider that their primary job is advocacy – promoting and facilitating an understanding of security considerations and the adoption of security best practices. Security advocacy necessitates a different set of competencies beyond the technical skills possessed by most security professionals. Non-technical competencies – such as interpersonal skills, communication skills, an appreciation of their audience, a customer-service orientation, and boundless creativity – may be essential for this role[4]. The security awareness team should also have a keen sense of the organization and its workforce: their goals, culture, constraints, and skill levels. Armed with this contextual knowledge, advocates then need to tailor security awareness communications and translate technical concepts into a language best understood by the workforce. This may require different messaging to the various roles within the organization.

> *If you're a computer scientist, and all you know is the computer science, and you don't have the empathy, you don't have the skills to listen,...you don't have that psychological side, I don't think you can make it work.* (usable security advocate talking about what it takes to do security advocacy well)

Building a multi-disciplinary team can be particularly valuable. In addition to those who understand the technology, programs should also leverage the talents of those possessing much-needed skills in communications, marketing, behavior change, event planning, and graphic design. In addition, if resources are an issue, consider having liaisons who are members of different organizational groups to serve as extensions to the team.

Make Security Relatable

Employees need a reason to care about security. Training should communicate the business value of security best practices to the organization: how it enables mission, assures revenue, or protects assets and reputation. Framing the importance of security awareness training in business terms can be especially important for gaining management buy-in. But, perhaps most importantly, people will be more apt to thoughtfully make security decisions when they have a sense of personal responsibility and view security as relevant to their day-to-day lives. Therefore, security awareness training should show the linkage between security and the duties of all roles in the organization, from front-line staff to senior executives.

Security communications should be topical, whether that be related to contemporary topics in the news, pressing organizational issues, or seasonal activities. For example, one federal agency has a December training event that educates the workforce on holiday-relevant topics such as safe gift shopping, including security and privacy considerations for smart home devices, interactive toys, and fitness trackers.

Another recent trend in security awareness training is an increasing emphasis on the work-home connection. With more employees teleworking in some capacity, they need to stay vigilant no matter their location. Good security habits are easier to form when they permeate someone's entire life and do not just end when they leave the office or turn off their work computer. To highlight this connection, in addition to topics of interest related to secure work habits, consider providing information employees can take home to educate their families, for example, on secure use of smartphone apps and social media.

Get Their Attention

In order to engage the workforce and reinforce training concepts, the security awareness team should go beyond the typical, once-and-done canned presentations to disseminate security information using a variety of communication channels and techniques periodically throughout the year. For example, we have seen organizations bring in high-quality speakers for security day events, produce concise handouts with security tips, hold security information fairs, create visually appealing posters, and enable remote broadcasting for those who cannot attend training events in person. Whatever the media, the approach should pique interest while being mindful of employee limitations on time, interest, and skill level.

> *You want to just put a different spin on it because people just see stuff all the time: "Have a good password. Lock your computer"…Be creative and think outside the box.* (security awareness professional)

Security awareness training should ideally be tailored to the local culture of the organization, be memorable, and be entertaining when appropriate. In our studies, we have come across numerous examples of creative approaches: a security-themed food truck event, complete with security trivia games while patrons wait in line to order; security-themed coloring books and calendars; a Shakespeare-themed play entitled "To send or not to send" that educated employees about proper email use; and a late-night show parody with a cyber-themed comedic monologue and guests who talked about security topics. Employing a variety of communication methods provides something for everyone, since employees will have different preferences on how they receive and best retain security-awareness information.

Empower Them with Tools

Raising awareness of security threats is important, but it does not necessarily lead to behavior change. Doing so without advice or appropriate tools on how to confront those threats may leave employees feeling anxious, unsatisfied, and powerless. Therefore, employees should be provided with practical, prioritized, and actionable steps they can take to protect themselves and their organization.

When providing recommendations, meet people where they are. Training topics should include recommendations that are achievable given employees' skillsets, described in terms they understand, and accompanied by pointers to helpful resources. Remember that "perfect security" is an impossible goal. Security is more of a journey, so start off by giving employees small steps they can immediately implement that have a large impact.

Measure Impact

Once this evolved security awareness training is in place, you need to determine if it actually makes a difference. Compliance metrics are easy to collect and analyze but are only part of the story. Unfortunately, it can be difficult to develop meaningful measures of aspects that matter most to your organization. To get you started, we suggest a few approaches that other organizations have found helpful.

If in-person or remote training events are held, attendance can be an indicator of reach. But be careful to not just focus on the numbers; also look at who is attending. This can lend insight into those buying into the importance of training, whether your program is reaching the right people, and where additional effort should be focused.

Employee feedback is another way in which you can quantitatively and qualitatively assess the effectiveness of your program. Informal break-room conversations are valuable, but anonymous, post-event surveys reach a broader audience and provide more structured, honest data. It is important to note though that response rates can be low and often are subject to self-selection bias. For instance, only those with strong positive or negative opinions may respond. Still, these can help the team gauge overall satisfaction, track perceived takeaways, and identify suggestions for future topics or formats.

Perhaps the most telling measure of effectiveness, though, comes in the form of trends in user-

generated security incident data aggregated from multiple sources. For example, after security awareness training regarding the sending of sensitive information via email, are the number of personal data disclosures going down? Don't just focus on where employees fall short; look at indicators of positive behaviors as well, for example increased reporting of suspicious emails or other security incidents to the help desk.

This holistic approach requires two-way communication with the cybersecurity and incident handling arms of the organization. Collaboration with physical security staff can likewise offer interesting insights into security mechanisms that have physical components, for example, smart cards used for both facility access and computer login. These partnerships have an added benefit: common threats to the organization observed by other security groups can help inform areas that may warrant additional workforce awareness and training.

> *We're trying to…be able to tie in together the people who take their training to the people who get caught with phishing exercises…with people who are losing their badges to people who send out information they shouldn't to see what's the correlation here. Are these people just too busy? Are they not paying attention? Is there a training problem?* (security awareness team lead)

Finally, since we all know that statistics can be misleading, be sure to contextualize the data you collect and consider possible explanations with targeted solutions. For instance, if a particular department within the organization is more susceptible to certain security threats, how can that population be better trained? If click rates (number of people falling for a simulated phish) for phishing training exercises go up one month, were the phishing emails more sophisticated than usual or was the email premise more aligned with the functions of the organization?

Be Positive and Constructive

At some point, all employees will have a security slip-up, and they usually hear about it! But what about commending them when they do something good? The threat of negative consequences has been found to have limited impact on decisions to implement security[5], but positive and constructive feedback can be effective in encouraging and maintaining desired behaviors[6]. To better incentivize employees to learn from their slip-ups, take an educational rather than a punitive approach when something goes wrong. Also try to recognize employees who make good security decisions, for example those who report suspicious emails or promote security best practices to their colleagues. Recognition doesn't have to be anything big. Sometimes a simple, but personal, "thank you" can be enough.

Strive Toward Continuous Improvement

You will likely not get security awareness training "right" from the start. Therefore, you should commit to improving the program incrementally over time. To ensure training stays fresh and keeps up with relevant threats to the organization, consider regular updates to your training material. This includes not just changes to topics, but also letting measures of effectiveness inform any necessary adaptations of communication channels to better accommodate employees and reach broader populations within the organization.

Finally, an organization's security awareness program should not be an island. Learn from others. Talk to security awareness professionals working in similar organizations about what works for them. Consider participation in online security awareness communities, which can be a wellspring of valuable resources (e.g., SANS[7], EDUCAUSE[8], and National Cyber Security Alliance[9]). Ideas can also be found at events that are focused on or have tracks related to security awareness training, for example, the annual Federal Information Security Educators[10] or RSA[11] conferences.

For cybertrust, there are baseline benefits of mandated security awareness training. However, organizations should be cautious about the potential pitfalls of slipping into a strict compliance mentality. Compliance metrics do not tell the whole story and fail to measure effectiveness of the program in sustained change in employee attitudes and behaviors. While compliance-based training is a start, security awareness programs should strive to go beyond – engaging and empowering employees to be informed, responsible cyber citizens in and outside of work.

Disclaimer

Any mention of commercial products or reference to commercial organizations is for information only. It does not imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the products mentioned are necessarily the best available for the purpose. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of their employers. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright annotations thereon.

References

1. https://csrc.nist.gov/glossary/term/Awareness_Training_and_Education_Controls
2. SANS. *2018 Security Awareness Report*, 2018, https://www.sans.org/security-awareness-training/reports/2018-security-awareness-report
3. J. M. Haney and W. G. Lutters, "It's Scary…It's Confusing…It's Dull: How Cybersecurity Advocates Overcome Negative Perceptions of Security," *Proceedings of the Symposium on Usable Privacy and Security*, 2018, pp. 411-425.
4. B. Woelk, "The Successful Security Awareness Professional: Foundational Skills and Continuing Education Strategies," 2015, https://library.educause.edu/~/media/files/library/2016/8/erb1608.pdf
5. H. S. Rhee, C. Kim, and Y. U. Ryu, "Self-efficacy in information security: It's influence on end users' information security practice behavior," *Computers & Security,* vol. 28, no. 8, 2009, pp. 816–826.
6. C. Hadnagy and M. Fincher, *Phishing Dark Waters*, Wiley, 2015.
7. https://www.sans.org/security-awareness-training/resources
8. https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/awareness-campaigns
9. https://www.stopthinkconnect.org/resources
10. https://csrc.nist.gov/projects/fissea
11. https://www.rsaconference.com/

Vita: Julie Haney *is a computer scientist and usable security researcher at NIST. Contact her at julie.haney@nist.gov.*

Vita: Wayne Lutters *is an Associate Professor in the College of Information Studies at University of Maryland. Contact him at lutters@umd.edu.*