HELP
SOURCE
Q&A

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/2WAF9G8

Q We are a multinational service organization that operates in multiple countries, hence, in different cultures. We have an online cybersecurity awareness program disseminated through the intranet. During a recent conference, a speaker stressed building a cybersecurity culture across the organization. As a security manager, how can we build a cybersecurity culture?

A Cybersecurity—or information security, as it used to be called—is a function of risk management. Security managers need to identify and evaluate risk that compromises the security of information assets. Implementing cybersecurity requires a very good understanding of the business, its risk, its strategy and its objectives. It also relies on a thorough knowledge of appropriate technology and supporting processes being used in the organization; skilled and competent people within the organization; and expertise leveraged from external sources when the needed skills are not available internally. Vulnerabilities exist in all components (people, process and technology) of security implementation. Vulnerabilities at the technical and processes levels can be fixed by tweaking processes, and vulnerabilities at the technology level can be mitigated by understanding system limitations and implementing solutions. However, vulnerabilities related to people can be addressed only by continuous awareness training. People include all those involved in executing business and security processes.

Although the security manager is the individual in charge of defining and implementing the security program, information security is the responsibility of all stakeholders of the organization. The concept of three lines of defense for securing information identifies employees involved in executing business processes as the first line of defense; they can detect when something is not normal. To ensure that they can recognize and report such abnormalities effectively and efficiently, they need security awareness training. Thus, appropriate training for all stakeholders is the first step in building a cybersecurity culture within an organization.

In October 2018, ISACA® and the CMMI Institute published a cybersecurity culture report titled "Narrowing the Culture Gap for Better Business Results."[1] According to the report, only 34 percent of organizations are aware of the role of cybersecurity culture in fostering cybersecurity within the organization. The report describes the cybersecurity culture as:

> *Cybersecurity culture is a workplace culture in which security awareness and behaviors are seamlessly integrated into everyone's daily operations, as well as a strategic executive leadership priority. In a threat-ripe environment, an effective cybersecurity culture can help employees understand their roles and responsibilities in keeping their organizations safe and customer data secure.*[2]

According to a blog by Tony Sager of the Center for Internet Security (CIS), culture is based on shared attitudes as well as written and unwritten rules that develop over time. Given the complexity and rapid changes that are associated with cybersecurity, culture plays an essential role, maybe even greater than any written policy or rule.[3] A similar level of complexity and rapid changes exists in the business and technology environments, so security culture plays an equally critical role in effectively securing the information assets of the organization.

Almost all cyberattacks have one thing in common: They thrive on human error, intentional or unintentional. Organizations can greatly minimize exposure by developing a security culture.

Many organizations do focus on awareness training, but it is often considered the responsibility of IT or the chief information security officer (CISO).

Sunil Bakshi, CISA, CRISC, CISM, CGEIT, ABCI, AMIIB, BS 25999LI, CEH, CISSP, ISO 27001 LA, MCA, PMP
Has worked in IT, IT governance, IS audit, information security and IT risk management. He has 40 years of experience in various positions in different industries. Currently, he is a freelance consultant in India.

Cybersecurity is not only the CISO's problem, it is the collective responsibility of the entire organization. Everyone must understand it. Building a security culture is more than just awareness; it requires behavioral changes.

A good example is the use of mobile devices. Many organizations have adopted bring your own device (BYOD) strategies. As a result, use of personal devices in the workplace is increasing and, if not handled appropriately, these devices can introduce vulnerabilities. This illustrates why awareness creation alone is not enough to ensure "cyberhygiene."

Security policies, procedures and technologies do help build a secure infrastructure, but that infrastructure is used and maintained by people. Not everyone in the organization can be a technology expert, but they are potential targets for cybercriminals. Therefore, it is important to develop a culture of cybersecurity that includes awareness, but also guides people's behaviors. The culture should encourage and support people "doing the right thing" and make it less likely that they will make mistakes.

How can an organization strengthen the cybersecurity culture? It can:

- Adopt global best practices to develop security strategy and policy
- Implement a strong risk management program that involves end users
- Ensure support from leaders, who lead by example. This goes a long way in strengthening the security culture.
- Be sure that security awareness material is not limited to only "dos and don'ts," but also includes answers to "why"
- Involve all employees by introducing a reward program for identifying new threats and reporting unusual activity
- Conduct social-engineering drills to observe the behavior of end users and communicate the results, then conduct training on changes to behaviors as needed

The focus of security culture, as described in this list, is to foster behavioral changes among users, not simply raise awareness.

Organizations that have implemented a cybersecurity culture have experienced benefits such as[4]:

- Increased visibility into potential threats
- Reduced cyberincidents
- Post-attack resilience to resume operations
- Increased capacity to engage in new business
- Consumer trust in their brand offerings

> "SECURITY POLICIES, PROCEDURES AND TECHNOLOGIES DO HELP BUILD A SECURE INFRASTRUCTURE, BUT THAT INFRASTRUCTURE IS USED AND MAINTAINED BY PEOPLE."

This point can be effectively concluded with a quote from Steven J. Ross:

> *Most people do not enjoy being told what they cannot do, even if they know they should not do those things. When security is framed as trust, consistency, reliability, predictability and productivity, it becomes easier to enlist others in a culture-strengthening exercise.*[5]

Endnotes

1 ISACA®, CMMI Institute, "Narrowing the Culture Gap for Better Business Results," USA, 2018, *https://www.isaca.org/info/cybersecurity-culture-report/index.html*

2 ISACA, "Nine in 10 Enterprises Report Gaps Between the Cybersecurity Culture They Have and the One They Want," 15 October 2018, *www.isaca.org/About-ISACA/Press-room/News-Releases/2018/Pages/ISACA-and-CMMI-Institute-Study-Reveals-Cybersecurity-Culture-Gap.aspx*

3 Sager, T.; "Developing a Culture of Cybersecurity With the CIS Controls," Center for Internet Security, *https://www.cisecurity.org/blog/developing-a-culture-of-cybersecurity-with-the-cis-controls/*

4 *Op cit* ISACA and CMMI Institute

5 Ross, S. J.; *Creating a Culture of Security*, ISACA, USA, 2011