What do Organizations Need to Build a Security Minded Culture?

by Larry Cates, President and CEO, Global Learning Systems

As many organizations struggle with ongoing phishing attacks, data breaches and lapses in physical security, they continue to wonder why employees are making poor security decisions despite the availability of training. The answer is that merely offering security training once or twice a year doesn't build the habits, mindset and motivation needed for employees to care about protecting the organization.

Instead of offering "check the box" training, organizations of all sizes should look at continuous learning programs that focus on building users' ownership and responsibility for safeguarding the organization's data and IT assets. That sense of ownership and responsibility is one component of a security-minded organizational culture.

At its simplest level, organizational culture is the sum of everything that affects what and how things get done in the business, including: organizational strategy; the behavior of leaders and how well they communicate their vision; and the values, attitudes and behaviors of employees. A strong organizational culture is rarely an accident — it's pursued intentionally and cultivated with purpose.

Security culture focuses on the shared recognition that security issues are an integral part of every employee's job. It fosters practicing good security habits and rewards security-minded decisions. Security culture is about instilling patterns of behaviors, values, attitudes and beliefs that support protecting organizational assets.

At its foundation, any thriving culture relies on behaviors. For a security culture, individuals must adopt the behaviors that protect the organization and learn specific skills that enable them to make smart security decisions. Once a baseline of skills has been achieved in security, phishing and compliance topics, a training program can dive more deeply into areas that target specific roles or pertain to a particular industry.

For a security culture to take hold, there need to be structures within the organization to support it. These structures include:

- Established avenues for two-way communication
- Regular review and maintenance of policies and procedures
- Strong IT infrastructure to automate security whenever possible
- Visible leadership by example
- Integration of security into organizational goals
- Employee performance objectives that include security practices

To be successful, a security awareness program should take a multifaceted, phased approach to changing behavior by using communication, training and assessments. When done properly, a continuous security awareness program helps build and maintain security culture by educating and motivating the individual, while also engaging the organization in dialogue, establishing norms and appealing to the natural human need to conform socially.

Larry Cates is the President and CEO of Global Learning Systems, a leading provider of security awareness and compliance training solutions for organizations of all sizes. Larry advises and consults with GLS customers on the design and implementation of continuous learning and behavior management programs. Prior to joining GLS, Larry held executive positions in corporate finance, development and operations w ith leading national homebuilders. He is a former US Marine Corps officer and a graduate of the United States Naval Academy.

Larry can be reached at lcates@globallearningsystems.com and at our company website, globallearningsystems.com