Your Employees Are Your Best Defense Against Cyberattacks

An Acumen article

2022

ACUMEN

seniormanagementworldwide
leading global provider of interim executives

We recommend the following six strategies to fortify the human firewall against the deceptive techniques of criminals and foster a security-aware organizational culture.

1. Ask employees to sign a security policy

Demonstrating commitment, such as signing a code of ethics, makes people more likely to follow through and leads to greater cognitive and behavioral adherence with codes of conduct. These policies are written commitments that state an employee will, for instance, treat all sensitive corporate information (e.g., customer and contractual data) confidentially, proceed in the best interest of the organization during on- and offline activities, and report suspicious incidents immediately to the respective internal point of contact. Employees also acknowledge that they will not disclose any sensitive corporate information to any external parties.

For example, CISCO requires its employees to annually sign a code of business conduct that reminds them how to protect the company's intellectual property, as well as confidential information assets. The company requires that its employees not share confidential or proprietary information with people who have no legitimate business need for it and to commit to reporting any observed breaches of such requirement. A corporate culture of blame can discourage employees from reporting suspicious activities, but ensuring they understand the rationale and asking them to sign a policy that signals their responsibility to report suspicious activities can circumvent this issue.

2. Lead by example

In situations of uncertainty, people look around them for cues on how to think and act. On the one hand, this behavior can be framed as conformity, but on the other, it can be seen as a way to help people grasp a common understanding of correct or normative behavior.

Looking to others for cues helps to reduce uncertainty — especially when those others are in respected social positions.

For instance, they should emphasize the importance of security behaviors like not leaving one's PC unlocked, not holding open doors at company site to people without verifying their legitimacy, and not exposing company documents, be they physical or digital, in public spaces. We recommend that leaders also provide contrasting examples of security-violation incidents where either they themselves had been careless or where careless behavior was reported. Doing so will help reduce the "it won't happen to me" feeling of invulnerability amongst the employees.

3. Elicit reciprocity

There is a pervasive social norm that dictates if someone gives us something, we feel obliged to return the favor. This urge tends to be true even if the original gift was not requested or even if what is requested in return is far more valuable than what was originally given. The norm of reciprocity is important because often the returned favor is done unconsciously.

Senior leaders should be aware of this powerful influencing technique and use it to strengthen a security-aware culture in the organization. Taking moves to secure an employees' own data or identity, like providing them with secure and encrypted flash drives or with a customizable digital photo frame that displays security reminders can be meaningful first steps to elicit reciprocity.

4. Leverage scarcity

People find objects and opportunities more attractive if they are rare, scarce, or difficult to obtain. Senior leaders can make use of this psychological tendency when promoting the organization's rare and exemplary security accreditations, such as accredited information security processes (e.g., ISO 27001), that stand to be jeopardized by a security breach.

By doing so and unequivocally communicating to the workforce both the organization's attractiveness as a great place to work due to the security culture, as well as what would be at stake were its security to be compromised (i.e., what one could potentially lose), senior leaders will strengthen employees' commitment to a security culture. Moreover, senior leaders should promote the installation of a classification system that separates innocuous from sensitive information. Employees will acquire a sense for the scarce — must-be-protected — information, which keeps them attentive in competently protecting the holy jewels of the company, instead of the illusionary task to protect all information regardless of its criticality.

5. Be like those you lead

Security professionals emphasize the importance of an empathetic mindset for achieving compliance in interpersonal situations. People are most influenced by others with whom they identify and like, and leaders can build trust with the workforce when they act with humility and empathy. Leaders who show vulnerability are likely to receive empathy and sympathy in return. This reciprocal exchange can indirectly foster compliance with senior leaders' directives in terms of ideal security behavior. Sharing their own struggles or storytelling about their own mistakes related to a security culture and how they learned from these mistakes can make them more approachable and identifiable, thereby increasing the chances that others will follow their lead.

6. Leverage the value of authority

Usually, organizations oblige their employees to take an annual digital security training. There is the real risk that employees click-through the activity but don't connect the contents to their daily behavior. When senior leaders, who employees see as the ultimate organizational authority, personally instruct their workforce to comply with corporate information security, they will be more likely to get the desired outcome. But there's a catch: Leaders need to be seen as a trusted source in addition to being the boss. It's the difference between merely being "in authority," ordering the workforce what to do, and being perceived as "an authority," knowledgeable of the topic. Having both is the most effective combination.