The human side of cybersecurity:

Ideas to help empower your employees and protect your organization

Cybersecurity is no longer solely the responsibility of technology experts—it's everyone's job. As a leader at your organization, you can play a critical role in helping to increase cybersecurity by raising awareness among employees. Through recruiting, hiring, training and day-to-day communications, you can help create a culture of cyber awareness and resilience.

Cybercrime isn't just technical—it's anti-social

Cyber criminals prey not only on systems and infrastructure, but also on people. One of the most common techniques they use is called "social engineering"—manipulating natural human tendencies to defraud a victim. By manipulating people's emotions, cybercriminals can successfully obtain user login credentials that open the door to whatever assets they want to destroy or steal. This typically means taking advantage of someone's feelings of fear, guilt, reciprocity or politeness to gain access to data that may be protected by a firewall or other means.

Educate employees to create a culture of cybersecurity

One of the best ways to combat a high-tech cyber threat is to start low-tech: with people. The antidote to social engineering is a culture of cyber awareness. Train and empower individuals to have a healthy skepticism about requests that have any warning signs of social engineering:

- An unknown caller asking for contact information of another employee
- An unexpected email urging the recipient to click a link
- A stranger trying to connect via social media
- Any requests to log in or supply their user IDs or passwords

Note that the most effective cybercriminals are chameleons—their emails may look like they come from legitimate sources or they may even seem to have social connections in common with their "targets." But they know their identities won't hold up to closer scrutiny, which is why they create false urgency to make people respond immediately.

Hitting pause may stop a cyberattack

Encourage employees to pause if they spot any of the situations above—even if their helpful attitude or emotional reactions might lead them to do otherwise. Make it clear: If an employee has any inkling a request seems suspicious, it's okay to slow down and verify the source.

In many cases, this can be done quickly through a simple check of an online search engine. A two-minute delay could either prevent a cyberattack or at least bring peace of mind.

Remember, you're not alone

Leaders from various departments (from HR, to Information Technology, to Legal) can help their organizations manage cyber risk within their own span of control, but they'll get even better results if they also work together. Partnerships across teams can help strengthen cybersecurity—and it all starts at the top.

Today's leaders set the stage for creating a working knowledge of cybersecurity among employees, which in turn helps their organizations prevent cyberattacks whenever possible, spot them when they do occur, and respond swiftly as needed.

Here's how:

- **Get the conversation going!** Advocate for putting cybersecurity on the agenda at leadership meetings so everyone can see what cyber risk means to their department.
- **Reassure IT professionals they're not alone.** Find and grow partnerships with in-house information technology teams, if they're part of your organization. Identify yourself as a champion of cybersecurity and see how you can help the effort.
- **Reach out beyond your organization's walls.** You may consider hiring experienced cybersecurity consultants, who can help assess — or put in place — systems infrastructure, policies and/or insurance protections to help round out your cybersecurity plan.

Learn more

We're committed to supporting your needs as a professional, as well as the needs of your organization and your employees. We'll do that by providing valuable insights into organizational trends and hot topics. And we want to hear from you. What keeps you up at night and how can we help? Please contact us!

- To learn how we can help you address the topics that matter most to your organization, starting with your retirement plan needs, contact your AIG representative or visit aig.com/RetirementServices.
- To learn more about cybersecurity best practices and solutions available, ask your AIG representative for a copy of our cybersecurity paper or visit www.aig.com/cyberedge.

Real strategies Let us put real retirement solutions to work for your organization and your employees

CALL 1-888-478-7020 **CLICK** aig.com/RetirementServices

VC 28438 (05/2019) J262103 ER