Strengthening Your Cybersecurity Through Team Training

October is Cybersecurity Awareness Month. While children may be hiding from witches and ghosts, compliance professionals have even scarier goblins to contend with: hackers and cyber thieves.

Cybercrimes are on the rise. Ransomware attacks on the Colonial Pipeline and JBS drew public attention to an issue those in the financial industry know all too well. The wealth of PII inherent in finance makes banks, investment firms, and asset managers prime targets for bad actors.

If you're a compliance officer, warding off cyber-scaries is a top priority. Fortunately, one of the most potent tools in your arsenal is all around you: your team.

Training your team to recognize potential threats and creating clear policies for reporting and escalating suspicious happenings can mitigate risks and protect your organization and your customers.

Create Clear Written Policies

Educating your team begins with clear written policies. It's not enough to say "cybersecurity matters." You must create guidelines for your team to live by. Identify what cybersecurity risks look like and how your team can reduce risks. Areas to highlight include:

1. The prevalence of phishing scams, malware, and Trojan horses

What red flags signal a potentially dangerous email? This warning from FINRA is a reminder that hackers exploit our natural desire to be helpful. Someone's first impulse may be to respond with requested information; your policies should encourage them to think critically before doing so.

2. The use of secure passwords and VPNs

Educate your team about creating secure passwords, using two-factor authentication, and logging in via VPN to prevent outside access to sensitive information.

3. The importance of regular software updates

Updates often address holes in the security of an application or operating system. Train your team to update all software regularly to ensure your defenses remain strong company-wide.

4. The role of vendor management in security

Any vendor that holds PII is a potential cyber risk, too. Create clear policies around vetting third-party vendors and maintaining secure connections between your data and their network.

Use Training to Test Teams

Once you've set your guidelines, put your team's knowledge to the test. Training modules with real-world examples are an engaging way to encourage your team to practice their risk-identifying bona fides. Some organizations even go so far as to send fake phishing emails or hire ethical hackers to put their teams to the test.

Regular testing is critical in building your team's muscle memory of what a swift, satisfactory response looks like.

Develop a Response Plan

What if your team does encounter a cyber-ghoul? The final piece of your training must ensure everyone knows how to act when faced with a real risk.

Create a place where employees can report incidents and escalate concerns. Whether it's sending an email to your compliance manager or submitting a form on your intranet, educate everyone on where to turn.

Should an attack occur, your team must also know how to respond. Define the steps they should take to:

- – Contain the damage
- – Keep your business functioning
- – Report the incident to requisite regulatory agencies and

customers, as needed

Establishing a plan in advance can keep a bad situation from becoming worse.

Get Everyone Involved

Reducing cybersecurity risks is a group effort. Your c-suite must be actively engaged in talking about cyber risks and championing policies to keep your data safe. Anyone—from your CEO to your receptionist—may spot a warning sign. Are you creating a culture where people feel empowered to report it?

Seek Out Training Opportunities

The training doesn’t stop within your four walls. Consider joining networking associations like NSCP and the IAA as a means to connect with industry peers and learn from their collective experiences. Fall conference season is here, and there are ample opportunities for topical education.

Compliance professionals may also set quarterly calendar reminders to undertake a periodic sweep of resources made available by the SEC and FINRA.

October is a spooky month, but with the right cybersecurity training in place, you can banish some of the monsters that may be lurking in the digital shadows. A well-educated team means your cybersecurity efforts are more likely to be a treat, rather than a trick.