What Does the CHRO Need to Know About Cybersecurity?

HR Dive | Jen Miller | August 29, 2024

"We have to stop looking at it as an IT problem," said Justin Miller, associate professor of practice at the University of Tulsa.

pixdeluxe via Getty Images

Cybersecurity remains a constant threat in the business world, with an all-time high of data compromises last year. It might be tempting to say that's not an HR problem, but cybersecurity isn't the sole domain of the IT department anymore. HR plays a critical role in both preventing attacks from happening, and responding if a bad actor gets in.

"We have to stop looking at it as an IT problem," said Justin Miller, associate professor of practice at the University of Tulsa.

HR departments can also be targets themselves, because of the vast amount of employee data they hold. It's "the motherload of personal data," said Miller. "They hold the keys to the castle to everything going on with every employee."

Here's what CHROs need to know.

Preparing people for cyber threats

CHROs play a critical role in defending against cyberattacks because of the popularity of phishing attacks, where hackers trick someone to either allow bad actors past normal cybersecurity walls, or impersonate someone to get an employee to do something they normally wouldn't do, like deposit money into a new account.

According to IBM, phishing is the most common data breach vector, making up 16% of all breaches. They're most costly too: IBM also found that phishing breaches cost an average of $4.76 million, which is higher than the overall average breach cost of $4.45 million.

"Most data security incidents are the result of human error, and human error means employees," said Peter Cassat, a privacy, data security, employment and technology law attorney and partner at Culhane Meadows. "If I'm a CHRO, I don't want to have that happening on my watch."

Anti-phishing training should fall under the purview of HR, just like other kinds of training do. That could mean running fake phishing campaigns to see how many employees fall for it. Cassat said some companies will also hold regular contests with prizes, challenging employees to spot what's wrong with an email — things like typos, incorrect headers and URLs.

The CHRO can also work to change the mindset of the role employees play in preventing data breaches and to "make it more visible and appreciated in the workplace," he said, and making cybersecurity part of the company's culture and mission.

Reacting in the event of an attack

Despite a company's best cybersecurity efforts, attacks still do happen, and some are going to be successful. According to the Identity Theft Resource Center, there were 3,205 data compromises — an all-time high — with over 350 million victims in 2023.

In the event of a breach, companies should already have an incident response plan in place, which dictates things like who does what in the process of minimizing the issue. That plan must include the CHRO, since that person "is uniquely positioned to communicate to the employee population," said Cassat.

If a problem is reported to a CHRO, especially if an employee thinks they've been phished, the CHRO should also be empowered to react immediately, said Miller, which might mean additional training in cybersecurity operations. That's far more effective than a CHRO working their way through an IT tree to get help.

"A lot of time is being left on the table. If you notice there's a cyber problem, [CHROs] need to be able to shut down those systems," Miller said.

Whatever works will depend on the company, and figuring that out involves breaking down silos between different departments to treat cybersecurity as the business-wide issue it is. "If you're

not willing to evolve in some sense to understand cyber, your company is going to be at risk," Miller added.