health payer
specialist

New Cyberthreat: Workers Burned Out on Passwords, 2FA, Security Rules

Many employees are weary of regularly changing passwords, dealing with multi-factor authentication or jumping through other security hoops to do their jobs.

By Ron Shinkman | March 19, 2024

As insurers rely on warehousing and managing enormous amounts of personal data for millions of policyholders, they find themselves at risk of cyberattacks that could harm their reputation, cost them business and spark lawsuits.

But they're also facing a threat that comes from inside, not outside: Their own workforces are growing numb to proliferating passwords that must be constantly updated, and a seemingly endless stream of requirements to adopt new cyber-safety measures.

The ongoing threats and the heightened vigilance that come with it has led to a form of security fatigue that could actually make insurers even more vulnerable.

"Employee security burnout is a material issue across all industries," said **Justin Somaini**, former chief information security officer at **Yahoo** and **Symantec** and currently a private equity executive in California. He added that workers have been worn down by IT requirements such as enduring multi-factor authentication for system logins, as well as the need to track documents shared with outside parties.

Security fatigue is usually more prevalent in the insurance sector than in other industries, according to **Mike Scott**, chief information security officer for **Immuta**, a Boston-based firm that provides security platforms for large businesses. That's not only because insurers must manage huge volumes of data, but also due to the fact they have legacy systems that have been used for decades, with many overlaid patches and changes throughout the years.

The result is a lot of disparate information technology systems, Scott said. "A lot of users are struggling with how getting into one system is different than accessing another system."

There can also be overly complex mechanisms to gain access to systems, particularly as more insurers migrate data from mainframe computers to the cloud. And insurance is an industry more highly regulated than most others.

"It's at a point where I think all (IT) users in insurance are getting inundated with a lot of things that other industries don't necessarily have to have," Scott said.

At the same time, cybersecurity has never been more important. Just in the past few weeks the insurance sector has been rocked by two hacks. A ransomware attack on **Change Healthcare**, one of the largest clearinghouses for medical claims in the U.S., essentially put that operation out of business for weeks. Change is also likely to lose a good chunk of this business to competitors, however several analysts say that may just be a short term phenomenon.

Another smaller attack was no less audacious: Hackers were able to access the records of more than 42,000 policyholders of **CNO Financial** after they were able to pull a "SIM swap" on the smartphone of a senior member of its executive team.

Tim Zeilman, a vice president and global product owner of cyber and privacy insurance for **Munich Re** affiliate **Hartford Steam Boiler** confirmed the problem exists. He said pressure points center around changing passwords and dealing with multifactor authentications.

"There are things employees deal with day in and day out, and it can get a little fatiguing at some point," he said.

Risks Are Compounded

Such fatigue can actually put institutions at significantly higher risk of a security breach.

"If employees become complacent due to burnout, the measures in place can actually work against the company's security," said **Kirsten Mickelson**, cyber claim practice leader at **Gallagher Bassett**, an Illinois-based firm that provides claim and risk management solutions to the insurance sector. "The more security measures in place, the less likely employees can keep up."

According to a 2021 survey by **1Password**, 30% of employees don't believe it's "worth the hassle" of getting permission from their IT department to obtain authorization to use specific software or applications. Moreover, 43% of employees are already employing easy-to-remember passwords at work that make infiltration more likely.

Meanwhile, IT professionals overseeing cybersecurity for large organizations are also in a dire state of their own, adding to the problem, according to **Stuart Madnick**, a professor of information technology at the **Massachusetts Institute of Technology**'s Sloan School of Management. Some of these workers are close to burnout, he noted.

"They're basically working around the clock," he said. That work overload can lead to security lapses and create vulnerabilities. According to 1Password, among IT employees who say they're experiencing significant levels of burnout, 44% say security rules and policies "aren't worth the hassle."

What Insurers Can Do

In response, carriers can't simply abandon their security efforts, or even ease off on the accelerator. But there are ways to make the layers of security more palatable for employees to negotiate.

They include issuing physical badges that can gain system access with a quick scan, mobile credentials that can be embedded in an employee's smartphone that accomplish much the same thing, or biometrics such as fingerprint or face or iris scans.

Zeilman noted that biometrics can be coupled with mobile credentials, as virtually all smartphones these days either scan fingerprints or faces for access. But gathering such information from employees and storing it in a database might be more fraught. "People tend to be particularly sensitive" about sharing such data with employers, he observed.

Other routes to avoid fatigue include gamifying security training. Hartford Steam Boiler doesn't take that approach, but Zeilman thinks it could work. Another way to address the issue: Clearer communications between IT departments and employees about why certain security measures are needed, and gathering input to make them more integrated with daily work tasks.

"I think a theme across this whole question is, 'How smoothly are they integrated? Is it a hassle to comply with those sorts of things?,'" Zeilman said. "Or is it relatively easy to do those in the course of your work life without a lot of extra work?"