Survey: Insider threats haunt security execs

Most organizations fail to confront or monitor employees prior to security breach incidents

While many organizations focus their security efforts on mitigating the threats posed by external actors, **some of their greatest risks come from within in the form of insider threats. From acts of violence to intellectual property theft, malicious insiders are of one the risks that keep security executives up at night and new research shows that companies are struggling to keep pace with the threat.**

According to a recent survey sponsored by post-hire screening services provider Endera and conducted by Vanson Bourne of 200 security executives at firms with more than 1,000 employees, companies, on average, were found to suffer at least three workforce-related incidents a week. More than half (55 percent) of the respondents reported that their organization struggles to limit the number of workforce-related security incidents and 44 percent said they were not aware of any potential workforce or personnel issues prior to an incident. Additionally, nearly 40 percent of those polled reported that their workforce had lost confidence in the organization's ability to keep them safe.

An overwhelming majority of survey respondents (87 percent) reported that contractors/freelancers are most likely to be the cause of a workforce-related security incident at their company, while two-thirds (64 percent) said that supply chain/third-party vendors were the most likely cause. For the purposes of the survey, Endera COO Steve Izurieta said the definition of "workforce-related security incidents" was kept broad and could range from major events impacting life safety and brand reputation to smaller incidents that could be mitigated with a simple conversation with an employee.

Among the top risks that security executives said their organizations were concerned about include, device theft or loss (86 percent), fraud (80 percent), cybersecurity threats (74 percent), and workplace violence and threats (55 percent).

Despite the concerns that companies expressed about workforce-related security incidents, Izurieta said they were surprised at how many organizations fail to do any sort of post-employment screening of its employees. In fact, according to the survey, while 75 percent of respondents said their organizations conduct background checks prior to employment, only 48 percent reported that these checks continue on a periodic basis.

"These were large organizations… and less than half of them are doing anything after the initial hire," Izurieta adds. "They may do something if there is an incident but that's an investigation versus an understanding of risk. They're not doing anything, so that's a lot of risk that is not being evaluated and therefore mitigated. A focus on that insider threat is really needed."

Raj Ananthanpillai, CEO of Endera, which was spun off two years ago from InfoZen and counts large financial institutions, healthcare providers and a global airline among its clients, says that though organizations spend copious amounts of money on physical and cybersecurity tools to protect their assets, they're woefully lacking when it comes to resources devoted to keeping tabs on potentially risky or criminal behavior by employees.

“An individual spends two-thirds of his or her time outside the enterprise. Companies put lots and lots of instrumentation within the enterprise in the form of cybersecurity, security monitoring, network monitoring, physical access, and so on but there is absolutely no visibility into what (employee) attributes and behaviors are outside the enterprise,” he adds

Among organizations that do conduct post-hire checks of their workforce, Ananthanpillai says what they commonly find is that while these companies have codified this process in their HR manual, many don’t exactly know how to go about actually monitoring for potential violations and are thus reduced to “hoping and praying” for people to self-report.

“I always use as an example – which is a true case that happened in a large franchise – is a childcare facility does a background check when a person is hired but then they go rogue and that person could be on sex offender’s list and the employer never knows about it until somebody does some post-hire monitoring,” Ananthanpillai says. “Think about the risk that poses to that facility, the children in that facility and the reputation of the enterprise.”

In this day and age of privacy concerns, Ananthanpillai says it’s also important that organizations tailor their screening efforts to look for red flags related to areas of specific, relevant risk as many companies have found themselves in hot water for delving into sources of data many consider to be off limits. Endera, for example, only looks at data that is in the public domain.

“The focus has to be on what is an actual risk for them,” Izurieta explains. “If it is just something that they would say, ‘Yeah, that’s nice to know but I’m not going to do anything about it,’ then don’t worry about collecting that information and then you stay away from the privacy piece. But, if it is something because of either their company policy or law because of regulation and they know about it, they have to take some sort of action. Action doesn’t have to mean termination, it could mean other factors but those are the things they should have mechanisms to understand and understand on an ongoing basis.”

SOURCE: Securityinfowatch.com, Article by: Joel Griffin, February 22, 2019