AMERICAN BANKER

Data-security lapses surge in work-from-home era

Penny Crosman

Penny Crosman

1064 words
16 November 2020
American Banker Online
AMBO
Vol.1, No.1
English
© 2020 American Banker and SourceMedia, Inc. All rights reserved.

Insider threats — the risk that employees will steal or inadvertently leak sensitive corporate information — are on the rise, partly because so many employees are working from home.

According to the Ponemon Institute, the number of publicly disclosed insider incidents has increased by 47% in two years, from 3,200 in 2018 to 4,716 in 2020. The research firm Forrester predicts insider incidents will increase another 8% in 2021. Companies are only required to publicly disclose data breaches when personally identifiable information is compromised, so the actual numbers are likely higher.

In a report published last week, Forrester analysts said three factors will produce a perfect storm for insider threats next year: the fast shift to remote work as a result of the COVID-19 pandemic, employees' job insecurity and the increased ease of moving stolen company data.

In the work-from-home environment, "you have more weak points for data exposure that could be caused by accidents," said Heidi Shey, a principal analyst of security and risk at Forrester.

At the same time, the cost of insider breaches is growing. According to Ponemon, the average cost of insider threats grew 31% from 2018 to 2020, to $11.45 million.

Financial services is among the hardest-hit industries. Shareth Ben, director of insider threat and cyber threat analytics at Securonix, which provides user- and entity-behavior analytics software to financial services firms, recently analyzed 300 insider incidents across eight industries. Financial services had the second-highest rate of insider breaches — 27.7% of the total (right after pharmaceutical and life sciences at 28.3%.)

"Anybody that works in the cybersecurity business knows we're in a riskier environment," said Gary McAlum, chief security officer at USAA. "The first reason is, you've taken a bunch of people that normally work inside facilities and now they're dispersed. So any benefit you have from physical access controls and management oversight has essentially gone."

The second, less obvious reason is that as people work remotely, as 98% of USAA employees are doing, "they want to be able to do exactly what they were doing when they were inside the building," McAlum said. For instance, they want to be able to print, and sometimes they print sensitive documents.

Employees are using personal devices to connect to corporate networks, without necessarily having the proper software security controls. They're using USB and Bluetooth data transfer devices unsupervised, McAlum said.

“Companies don't have a really good governance process for how they allow all of that,” he said. “You can start to lose sensitive information and data that way.”

USAA has a rigorous policy around who is allowed to print remotely.

“Just because you say, I need to print, that's not enough,” McAlum.

Another issue for people who can access sensitive information from home is, who else is in that home, McAlum noted.

“How is that information being protected? Who's looking over your shoulder?” he said.

Employees working from home are using the same Wi-Fi as other family members who might be downloading movies that might contain malware, pointed out MIT professor Stuart Madnick. They’re using new software tools, such as webinar and conferencing programs, with which they might not be familiar.

Another threat escalator is the fact that bad actors know that everybody's working remotely and have been targeting vulnerabilities in virtual private networks and stepping up their phishing attacks over the past eight months. Employees are more vulnerable to business-email-compromise attacks that appear to come from colleagues who are no longer down the hall. They’re also more susceptible to phishing attacks from emails that appear to have useful information about local COVID-19 cases and lockdown information.

At the same time, patching all the computer and phone endpoints in a remote environment can take longer than when they’re in common buildings, McAlum said. And employees are under more financial pressure, especially those with spouses out of work, which can help them rationalize improper behavior.

In the worst-case scenario, a person who has elevated data-access privileges is actively looking to steal or do something malicious, McAlum said. But plenty of times, insider threats are inadvertent.

Wade Lance, chief technology officer at Illusive Networks, estimates that 60% of insider threats are unitentional data leakages, policy violations, data exposure or data-loss incidents. Illusive Networks’ software detects cybersecurity threats and tries to gather information and remediate; half its customers are in financial services.

Companies need to keep a close eye on people with data-access privileges, such as software developers, database administrators and systems administrators.

“It's a huge risk for that insider going rogue or for their system to be compromised so an external threat actor can leverage the capacities of that system,” Lance said.

Privileged users can accidentally click on phishing emails and become unwitting accomplices, for instance.

“An insider incident could be as simple as someone who got distracted sending an email and attaching the wrong file or typing in the wrong recipient name,” Shey said.

And there are negligent insiders: people who, in the course of trying to get their job done, circumvent existing controls out of frustration.

Not all employees are completely equipped to do their jobs from home, Shey pointed out.

“You have some people who start to go off and find free tools to use so they can remain productive,” she said. She has also heard of employees who do paper-based work moving filing cabinets full of records to their homes.

“To me, that's a bit of a nightmare in terms of how are you controlling access and use of this information and protecting it at that point?” Shey said.

Banks are doing several things to mitigate the insider threat: They're tightening controls around data access, monitoring access to data more closely through data-loss-protection and behavioral analytics, and educating employees about security.

Along with these stricter security measures, Shey recommends a softer approach: supporting employees more broadly during these tougher times, and therefore giving them less motivation to compromise data.

Companies that don’t do this “could inadvertently be setting up the conditions that are ripe for insider threats of the malicious kind, from disgruntled workers and people who feel like they're just a number.”

SourceMedia, Inc.

Document AMBO000020201116egbg000m9