AMERICAN BANKER.

5 ways banks can guard against internal cyber threats

Penny Crosman

Penny Crosman

1445 words
17 November 2020
American Banker Online
AMBO
Vol.1, No.1
English

Banks and other companies can take several steps to minimize the rising number of cybersecurity threats coming from within their organizations.

“Banks’ primary concern is they don't want to be on the front page of any newspaper,” said Shareth Ben, executive director of insider-threat and cyber-threat analytics at Securonix. He worked with Morgan Stanley after a 2014 insider breach in which one of its financial advisers posted information about 350,000 clients on the website Pastebin.

“Brand reputation is No. 1, and the second thing is mitigating any financial loss from actions from the [Securities and Exchange Commission] or other regulators," Ben said.

Experts recommend five deterrent measures: closely monitor privileged users, track data flows with special analytics tools, toughen security policies, offer employees more technical and personal support and teach them about security.Monitor privileged users

Many banks have been closely monitoring privileged users, such as network and database administrators, Ben said.

“They’re investing in monitoring technologies to make sure that the controls they put in place are indeed working,” he said.

They're also setting tighter controls for privileged and regular users. They have to be careful here, so that the restrictions don't prevent people from being able to do their jobs.

Gary McAlum, chief security officer at USAA, noted that one way banks can strike that balance is to by masking sensitive data.

“For people that have access to sensitive data, do they actually need to see it all? Or do they just need to see some part of it?” McAlum said.Deploy sensitive analytics

Data-loss-protection software has long been banks’ top technology answer to insider threats. DLP technology monitors who is looking at what data and identifies instances where data is moving around in ways that it shouldn't, when the people accessing it have no reason to.

One limitation of DLP is it’s rules based, McAlum said. A typical rule might state, for instance, that employees can’t email out files that contain a Social Security number. In the shift to remote work, the old rules don’t always apply.

“The baselines are all blown to pieces,” said Wade Lance, field chief technology officer of Illusive Networks. “Now people work weird times: They take their kids to school and come back.”

Another limitation to DLP is it's not plug-and-play — it requires a lot of implementation work and sometimes professional services from the vendor, McAlum said. A somewhat newer approach to identifying insider threats is user- and entity-behavior analytics technology.

“Everybody's looking more closely at UEBA,” McAlum said.

UEBA uses artificial intelligence to watch user behavior for anomalies. It might see an employee download a type of file he’s never downloaded before. It will then assess the level of risk to the information in that file.

“The promise is it starts to know over time what normal behavior looks like for each employee,” McAlum said. “And when something doesn't look quite right, it flags it.” There may be a lot of false positives early on, but over time the software should start to learn what normal looks like.

Heidi Shey, principal analyst at Forrester, also highly recommends UEBA software.

“It’s a smarter response to a policy violation because you're not just looking at how's the data moving, but you're also looking at what was this employee doing leading up to that?” Shey said.Set stricter security policies

Executives often make “semiconscious decisions” about security, said Stuart Madnick, professor at MIT.

“What I mean by semiconscious decisions is they'll say, well, I know I've left the back door open, or I left the key under the mat, and that probably isn't the best thing to do,” he said. “But I'm very busy right now, and it's taking me an extra five minutes to lock that back door. So I'll just let it go. And they don't realize that that decision could cost millions of dollars.”

For instance, in a study of the Capital One Financial-Amazon Web Services data breach , MIT researchers found the bank made 61 mistakes, Madnick said. News reports at the time painted the intrusion as a break-in to a misconfigured firewall.

Ariel Zeitlin, chief technology officer at Guardicore, a security company whose top client vertical is financial services, sees a movement in the financial services industry toward zero trust.

“The idea behind that is trust no one,” he said. And give no employees access to any data they don’t specifically need to do their job.

“Zero trust is making a lot of positives noise in organizations,” Zeitlin said. “People are understanding this is the right way to go, and there are technologies that can help manage this complexity and adopt zero trust across an organization.”

McAlum echoed this idea. Thought banks typically have data-loss protection and access controls, “a lot of times people don't turn all those on because it's a little bit more rigorous than people want. You should probably default to the rigorous versus the convenient in this environment.”Support employees, don't spy on them

Shey questions the benefit of productivity monitoring software to keep an eye on remote workers.

“Is this something that you really need?” she said. “At this point in time, can we be humans and treat our employees like they are adults who will do their job and get things done without someone looking over their shoulder to do that? Because that's just too much.”

Early on in the pandemic, Shey heard of companies that would take a snapshot through the video cameras on employees’ laptops every 30 seconds.

“That seems like overkill,” she said.

At one bank she worked with, an executive was pushing hard for employee monitoring tools and making employees sign attestations about how they're working or handling data. The human resources department pushed back and said that would end up hurting people and hindering employees from doing their jobs, and maybe give them ideas.

“You don't want to be treating your own employees like they're criminals,” Shey said. “That might be the last straw for somebody who's already stressed out and frustrated and scared at this time. It could help to turn employees into malicious insiders.”

Through coordination and collaboration with HR, companies should listen to and understand employees’ concerns about remote work, Shey said. When companies monitor their employees, they need to clearly communicate the purpose of that, so people understand what’s happening.

“It should not be a surprise to any employee,” Shey said.

But McAlum pointed out that in the regulated financial sector, there can be no expectation of privacy. Banks have to monitor employees for compliance and risk management purposes.

“It's not about trust,” he said. “It's about trust but verify.”

But he also pointed out that in security monitoring, “you don't have a security team sitting there reading everybody's email. The software looks for certain triggers and flags.”Teach employees about security

“Educating people, making them more aware is probably the best thing we can do,” Madnick said.

Bank employees should be taught, for instance, that if they’re on video camera, they should be aware of what may be in the background, he said. They should think before recording video meetings in which sensitive data is shared.They should be reminded not to use the default password on their videoconferencing accounts.

Traditional cybersecurity training tends to not work because people forget most of what they learned by the following day or at least the following week, Madnick said.

But peer pressure can work, he said.

For instance, workgroups could be told that if one person in the group falls victim to a phishing attack, everyone in the group will get a cut to their bonus. If two people fall victim, there will be zero bonuses for the group.

“That’s a rather draconian way of doing this, but it works,” Madnick said. The same idea could be carried out by praising the groups with the best security and safety record.

McAlum sees insider threats as an area that calls for continuous improvement rather than complacency.

“I think it's fairly safe to say that no company is going to go back to exactly the way they were before, McAlum said. “We see this as an opportunity to think through the future. What else can we do differently now? What could we be planning for as we look into the future?”

SourceMedia, Inc.