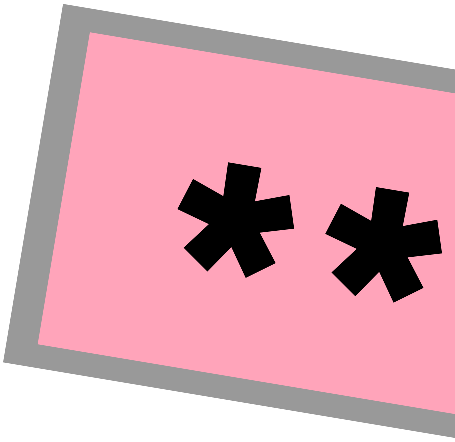
A Holistic Approach to Cyber Preparedness in Banking



By Wolcott Wheeler

Cyber criminals are getting increasingly aggressive. That's bad news for everyone, but particularly for banks. The banking sector is typically among the top three industries targeted by cyber criminals, fraudsters, and nation-state actors, according to Catarina Kim, intelligence group practice leader at Aon. In fact, Statista reported that financial services was the global sector most targeted by basic web application attacks for the 12 months spanning November 2021 to October 2022.

"While 2022 wasn't a great year for innovation when it came to malicious targeting, the volume of attacks against the financial services sector certainly made up for the lack of new or novel techniques by threat actors," said Kim, part of a recent RMA panel on cybersecurity trends and threats affecting the financial industry. The group discussed response preparedness, best practices, and how business models and culture can be engineered to create a holistic cyber-preparedness environment.

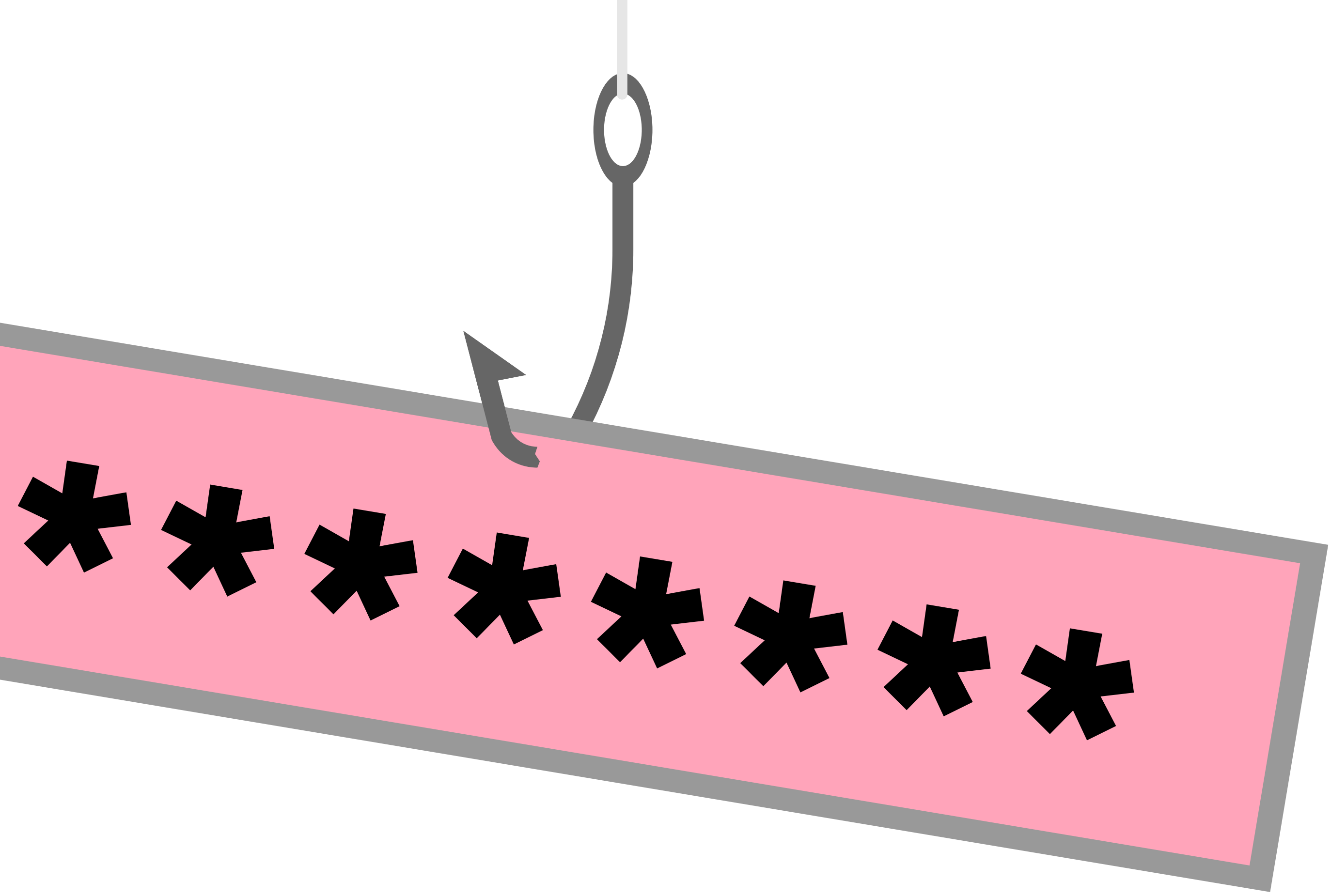
"In the wake of global incidents such as deep fake attacks targeting banks in Hong Kong, we've seen a lot of concern arise about financial stability," said Kate Kuehn, chief trust officer of cyber solutions at Aon. "We're very aware of how cyberattacks can impact the holistic architecture and infrastructure of the financial system."

Kuehn noted that banks continue to watch for and be wary of possible exploits related to NATO's support for Ukraine as it tries to push back the Russian invasion. On the one-year anniversary of the war, the U.S. Cybersecurity and Infrastructure Security Agency warned organizations in the U.S. and Europe that they still faced the possibility of "disruptive and defacement attacks against websites in an attempt to sow chaos and societal discord." Kuehn said nation-state activity can also "trickle down into commercial services." She said threat actors have taken "exploits that were put out into the wild and tried to deploy them against banks and other types of financial services" including cryptocurrency exchanges.

Kim emphasized that phishing and ransomware remain serious threats. They "pop up continuously and it seems like they will never go away despite companies investing millions of dollars into phishing training for their employees. Ransomware groups, in particular, have leveraged phishing campaigns to get access into banking networks by targeting their employees."

Kim also pointed out the threat of supply chain risks. "As banks have shifted to mobile apps and other third-party services and platforms that enhance banking, there is increased exposure to additional vulnerabilities," she said. It could be that "cloud environments are not configured correctly or perhaps apps are simply not built in a secure way."

"Due to poor encryption and other vulnerabilities, it has been very easy for some threat actors to get a foothold into third-party environments, which



can then impact larger financial services firms—and the services they provide to customers," she said.

Samantha Billy, U.S. broking growth leader at Aon, stressed the importance of "evaluating the risks your vendors have through your vendor management controls."

Another way a security weakness can be introduced, said Jonathan Rajewski, managing director and practice leader, Stroz Friedberg Digital Forensics and Incident Response Solutions at Aon, is when "developers add an attractive feature to their network" before the feature is "properly tested and vetted."

"Don't put it into production before it's safe," said Rajewski. The danger, he said, is that a bad actor who finds just one vulnerability in a line of untested code can get access to an entire network.

Bad actors are also trying to leverage the financial pressure employees may feel from recent mass layoffs across the banking and technology sectors to launch exploits. "Threat actors are preying on financial insecurity to recruit employees with access to sensitive information," according to Kim. She added, "We have observed a visible increase on the dark web of threat actor groups seeking to recruit insiders who have access to not only credentials but specific enterprise platforms. Companies should start thinking about not just how to protect their data from leaving, but also how to change the culture within a company so that people understand the inherent risks that may exist by having individuals going to the dark web and attracting a lot of very lucrative offers."

Billy stressed that employees should constantly be made aware of the seriousness of cybercrime's threat to the banking industry. "It's important to use training and education to bring cybersecurity awareness to everybody in your culture," she said.

Rajewski said banks would benefit from being proactive in identifying vulnerabilities and closing gaps, and stressed constant vigilance. For example, he said, even if a bank detects a vulnerability and patches it, a malicious actor may have already breached the system elsewhere. "Identify where the critical assets are and build layers of security around that," he said. "It can really help you in the long term if you can identify that threat as quickly as possible. It's also crucial that you have great backups that are properly segmented."

The organizations with the best success on the cybersecurity front "are being proactive," he said. "They're playing offense, not just playing defense. They're threat-hunting in their infrastructure. They're doing threat assessments. They're doing vulnerability management. They're thinking about that zero-trust resilience goal."

As a precaution, Kuehn advised: "Identify where cyber risk lives in your organization and understand the threats in each category. Then talk about your exposure from a threat perspective." Next steps, she said, include assessing the lengths the organization is willing to go to address the risk and considering solutions like cyber insurance to help mitigate and offset the exposure.Ⓡ