Under Siege From Cybercriminals

U.S. Financial Organizations Struggle With Attacks

If your company is in the financial sector, there is a 77% chance that your institution experienced a cyberattack last year. The average cost per attack in your industry was nearly $6 million—money that may not have to be lost if effective procedures were in place beforehand.

The financial sector of the world's largest economy—the United States—is not only trusted with the critical data and assets of its citizens; it forms one of the pillars of the nation's stability, as well as that of global economies. Trust in American financial institutions forms an integral part of their strength.

As the sector has increasingly relied on digital assets, banking technology has also opened new vulnerabilities and new attack vectors that can potentially erode that trust. The question now is whether the sector can keep up with, or stay a step ahead of, the future on its horizon.

The Vulnerability Factors

The financial sector attracts hackers attempting to steal funds, but others are after the troves of sensitive personal information that can be used for further attacks or extortion. Speaking to the Financial Times,[1] Steve Stone, head of Rubrik Zero Labs at security group Rubrik, noted that financial services organizations already hold 20% more data than those in other sectors. "More data means a larger surface area to target and more potential blind spots."

Luke McNamara, deputy chief analyst at Mandiant Intelligence, Google Cloud's cybersecurity business, adds that "entities within the financial sector" can also be a target for "espionage actors", such as nation states, because they play a role in "politically sensitive functions, such as sanctions enforcement and compliance, or financing of high-profile or controversial projects."

Today virtually every banking or financial transaction executed is done on a computer. The threat landscape has dramatically widened as American consumers and businesses have demanded, and become accustomed to, a 24/7 connection to their accounts through smartphones and retail payment processing. As of October 2023, 71% of Americans prefer to do their banking over mobile phone, tablet, or laptop[2]—meaning roughly 238 million people, with varying levels of awareness and ability to recognize a phishing email or attempt to compromise their credentials to access their accounts, can connect digitally to their banks any time of day and any day of the week.

The rapid technological adoption needed to meet this demand has brought increased reliance on external vendors, and a new level of digital interconnectedness with partners such as IT consulting firms and service providers. Infosys McCamish Systems, which provides services for deferred compensation plans including plans serviced by Bank of America, illustrated this in February 2024 when the company confirmed that a November 2023 breach of their systems has led to the compromise of personally identifiable information of more than 57,000 Bank of America customers.[3]

Today's Landscape

Unsurprisingly, as the attack surface and vulnerabilities widen, and the value of their data increases, cyberattacks targeting financial institutions are becoming more frequent, sophisticated, and destructive. In the first half of 2021, TrendMicro saw a staggering 1,318%

[1] Murphy, Hanna, "Cyber attacks reveal fragility of financial markets," Financial Times, January 16, 2024, site

[2] "National Survey: Bank Customers Use Mobile Apps More Than Any Other Channel to Manage Their Accounts," American Bankers Association, October 26, 2023, site

[3] Winder, Davey, "Bank Of America Warns Customers Of Data Leak Following 2023 Hack," Forbes Magazine, February 13, 2024, site

increase in ransomware attacks targeting banks and financial institutions compared to the same period in 2020.[4] While such extreme percentages have not been recorded in subsequent years, the surge in attacks against the financial sector has not abated.

In the early part of 2023, Corvus Insurance, which tracks hacker posts on the dark web, reported a 60% spike in successful ransomware attacks across industries compared to the same period the previous year. More unsettling, the company noted a 300% surge in strikes against financial services companies.[5]

By mid-2023, according to SOCRadar, the financial sector had already suffered more cyberattacks in six months than it had in all of 2022.[6] By the end of the year, 77% of financial institutions had been the target of an attack by cybercriminals.[7]

The costs to financial institutions from cyberattacks are among the highest in the world. Averaging $5.9 million per incident, the 2023 IBM Cost of a Data Breach report places the financial sector second only to healthcare in the cost of attacks. Financial institutions pay roughly $1.5 million, or 28%, more per incident than the average across all industries.[8] For what IBM deems mega breaches, those that involve the loss or theft of between one million and 60 million records, the costs soar to tens and even hundreds of millions of dollars.

The Adversaries Are Getting Better

The growing wave of attacks on the finance sector also illustrates an increasing ability of adversaries to consistently execute attacks against the sector at a rising scale. They have been helped by the development and refinement of the ransomware-as-a-service model, which has lowered the barrier to entry for would-be hackers, while attacks have also become more sophisticated, making the threat of ransomware following a social engineering attack arguably the biggest cyber risk facing financial services organizations today.

KnowBe4 founder and CEO Stu Sjouwerman notes in Forbes that generative AI “has introduced an alarming escalation of social engineering threats,” including the ability to draft increasingly sophisticated phishing emails without the irregular language and typographical errors that normally serve as red flags to users, and improved voice cloning making it possible, for example, to impersonate family members and con victims into transferring money to them on the pretext of a family emergency. With autonomous agents that can generate a systematic sequence of the kind of tasks that AI Large Language Models work on, Sjouwerman says, “threat actors can carry out highly targeted social engineering attacks at an industrial scale.”[9]

How Prepared is the Financial Sector?

In its 2023 Survey of Banking CEOs, KPMG noted that only 54% of respondents said they were well-prepared for a cyberattack, a slide from 66% in 2022. Those describing themselves as under-prepared rose to 21% in 2023 compared to 10% in 2022. When asked why they feel under-prepared for a cyber threat, 40% pointed to the increasing sophistication of attackers, 27% acknowledged a shortage of skilled personnel and 17% blamed a lack of investment in cyber defenses.[10]

[4] Poireault, Kevin, “Financial Industry Faces Soaring Ransomware Threat,” Infosecurity Magazine, July 12, 2023, site

[5] “Ransomware Attacks Remain High: April 2023 Takes Spot for Third Highest Month,” Corvus Insurance, May 18, 2023, site

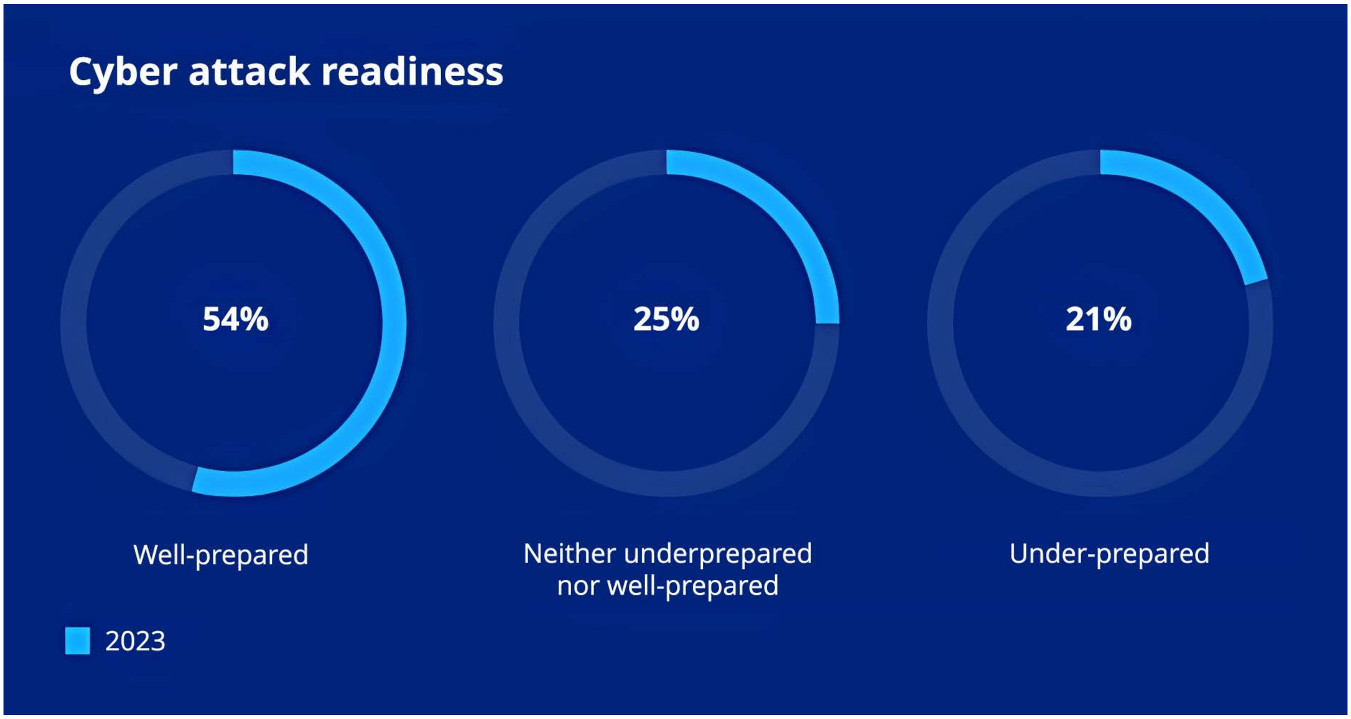
[6] Poireault, Kevin, *Infosecurity Magazine*

[7] “Netwrix 2023 Hybrid Security Trends Report, Additional Findings for the Finance and Banking Sector,” Netwrix, n.d., site

[8] “Cost of a Data Breach Report 2023,” IBM, site

[9] Sjouwerman, Stu, “How AI Is Changing Social Engineering Forever,” Forbes Magazine, May 26,2023, site

[10] “KPMG 2023,Banking CEO Outlook,” KPMG International, n.d., site



[11]

We can guess that JPMorgan Chase, the largest U.S. bank by assets, is one of the 54%. Speaking at the World Economic Forum in Davos, Switzerland in January, Mary Callahan Erdoes, head of asset and wealth management division for the company, said the bank now invests $15 billion a year and employs 62,000 technologists to fortify its defense against cybercrime.

“We have more engineers than Google or Amazon,” she said. “Why? Because we have to.
The fraudsters get smarter, savvier, quicker, more devious, and more mischievous.”

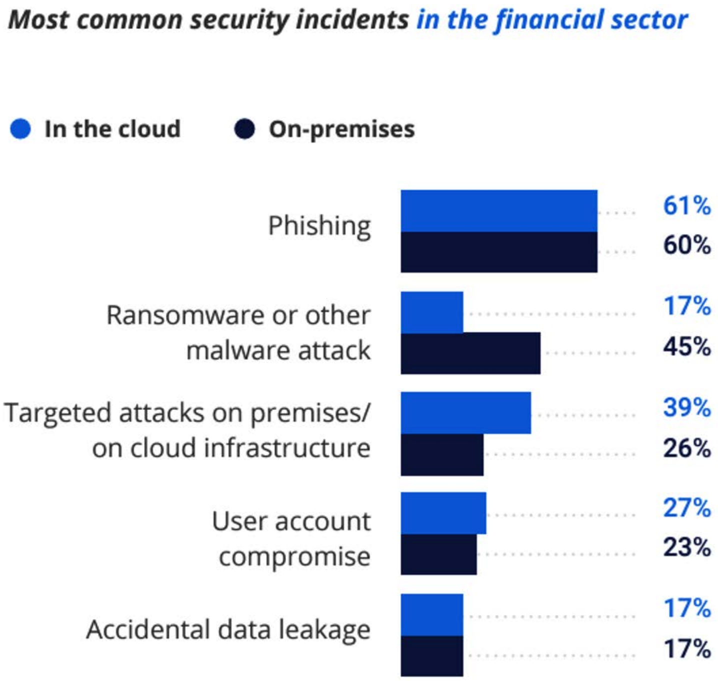
But it is the small banks that may be taking the larger relative hit, as they struggle to adhere to the same standards and regulations as the big banks, and face the same growing risks, with fewer resources and far less ability to attract the skilled personnel to respond to cyberattacks.

Phishing Their Way In

Phishing and social engineering continue to be the primary tool for gaining access to critical customer banking information and funds. This is not unique to finance; according to Verizon’s 2023 Data Breach Investigations Report, 74% of breaches across industries involved the human element, which includes social engineering attacks, errors or misuse.[12]

[11] “KPMG 2023,Banking CEO Outlook,” KPMG International

[12] “2023 Data Breach Investigations Report,” Verizon, site



But again, the financial sector appears to be one of the most targeted sectors. APWG's Phishing Activity Trends Report notes that 2022 was the highest year on record, with 4.7 million phishing attacks across industries. But 27.7% of those attacks targeted the financial sector specifically. In the second quarter of 2023, the financial sector continued to be the most-attacked sector, with 23.5% of all phishing attacks. Attacks against online payment services were another 5.8% of all attacks.[13]

In Conclusion

The financial sector is undoubtedly more susceptible to social engineering attacks and other cybersecurity threats due to the very nature of the services they provide which involve individual's wealth, financial means and other assets. They are also tasked with the enormous responsibility of protecting people's most prized and fundamental resources that they rely on every day to purchase food, shelter, medical needs and more. A breach of critical information can be detrimental to a financial institution's reputation and managed assets that are entrusted to them by their customers.

Protecting against cybersecurity threats in this new era of online and digital banking that can be done with a few simple clicks. It requires increasing awareness, maintaining a strong security culture and a focus on managing human risk. While cyberattacks remain steadfast, the financial sector in the U.S. must be persistently committed to safeguarding customer trust to uphold the solid foundation and reputation upon which this sector was built.

[13] "Phishing Activity Trends Reports," 2nd Quarter 2023, APWG, November 7, 2023, site

Additional Resources

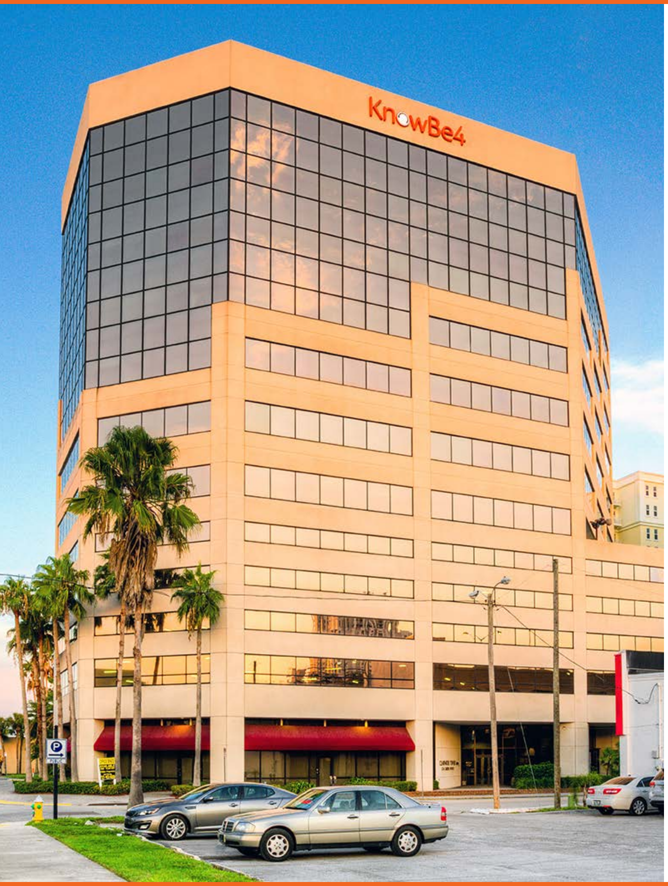
Free Phishing Security Test
Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

Free Automated Security Awareness Program
Create a customized Security Awareness Program for your organization

Free Phish Alert Button
Your employees now have a safe way to report phishing attacks with one click

Free Email Exposure Check
Find out which of your users emails are exposed before the bad guys do

Free Domain Spoof Test
Find out if hackers can spoof an email address of your own domain



About KnowBe4

KnowBe4, the provider of the world's largest security awareness training and simulated phishing platform, is used by more than 65,000 organizations around the globe. Founded by IT and data security specialist Stu Sjouwerman, KnowBe4 helps organizations address the human element of security by raising awareness about ransomware, CEO fraud and other social engineering tactics through a new-school approach to awareness training on security.

The late Kevin Mitnick, who was an internationally recognized cybersecurity specialist and KnowBe4's Chief Hacking Officer, helped design the KnowBe4 training based on his well-documented social engineering tactics. Tens of thousands of organizations rely on KnowBe4 to mobilize their end users as their last line of defense and trust the KnowBe4 platform to strengthen their security culture and reduce human risk.

For more information, please visit www.KnowBe4.com

KnowBe4
Human error. Conquered.

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com