KnowBe4

Financial Sector Threats:
The Shifting Landscape

WWW.KNOWBE4.COM

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

0625US

Table of Contents

INTRODUCTION

The security of the global business community rests on the stability and reliability of the international finance sector, stability that is in turn built on trust and an internationally recognized regulatory framework. When financial institutions are breached, the consequences can range from temporary disruption of services to loss of reputation and clientele, and worse.

Damage from an attack on a financial institution can cascade across the globe; a cyberattack in 2023, for example, on the U.S. arm of China's largest bank, the Industrial and Commercial Bank of China, temporarily disrupted trades in the U.S. Treasury market. The Federal Reserve Bank of New York estimates that, on average, if any of the large banks were unable to make payments for a day, up to 38 percent of the banks in their network will be impacted, including breaching their end-of-day reserves threshold.[1]

When criminals get access to stolen home addresses and bank balances, the results can turn deadly, with exponentially higher potential liability. Coinbase, the largest crypto exchange in the U.S., holds the world's most valuable Bitcoin deposits. On May 11, 2025, the company discovered a breach that had exposed names, addresses, phone numbers, email, Social Security numbers, masked bank account numbers, government ID images, balance and transactions of nearly 70,000 account holders. Coinbase estimates the cost of the attack at $180 - 400 million in remediation and reimbursements, but the company is also facing a flurry of lawsuits by users who were compromised.[2] TechCrunch founder Michael Arrington has suggested that, with kidnapping of crypto investors and their families on the rise, the company should be held accountable for having put the lives of Coinbase investors at risk.[3]

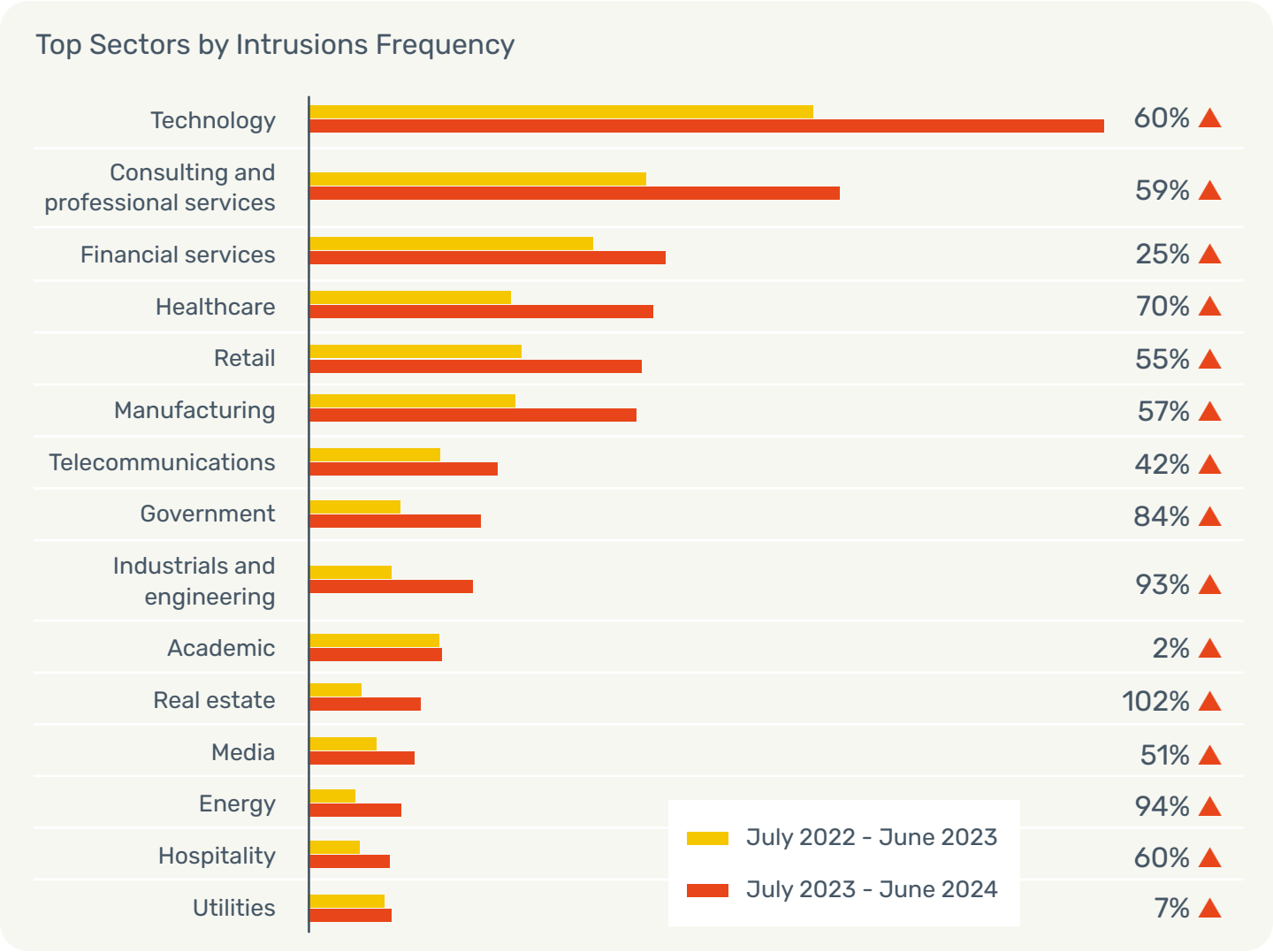
1 Eisenbach, Thomas, Kovner, Anna, Junho Lee, Michael, "Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis," Federal Reserve Bank of New York Staff Reports, May 2021, https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr909.pdf
2 Quill, Vince, "Coinbase breach hit almost 70k users – Attorneys," Cointelegraph, May 21, 2025, https://cointelegraph.com/news/70k-impacted-coinbase-data-breach-maine-attorneys
3 Maruccia, Alfonso, Coinbase hack could get people killed, TechCrunch founder warns," May 21, 2025, TechSpot, https://www.techspot.com/news/108009-coinbase-data-heist-could-have-deadly-consequences-techcrunch.html

The Six-Year Surge

In 2019, the Boston Consulting Group noted that financial service firms were experiencing up to 300 times more cyberattacks per year than other firms.[4] In the first half of 2020, as COVID-19 changed the commerce landscape, overall cyberattacks targeting financial institutions increased by more than 238%. The increase in ransomware attacks against the financial sector was even more alarming, with 900% growth from the beginning of February to the end of April 2020. 82% of surveyed financial institutions said cybercriminals were also becoming more sophisticated in their attacks.[5]

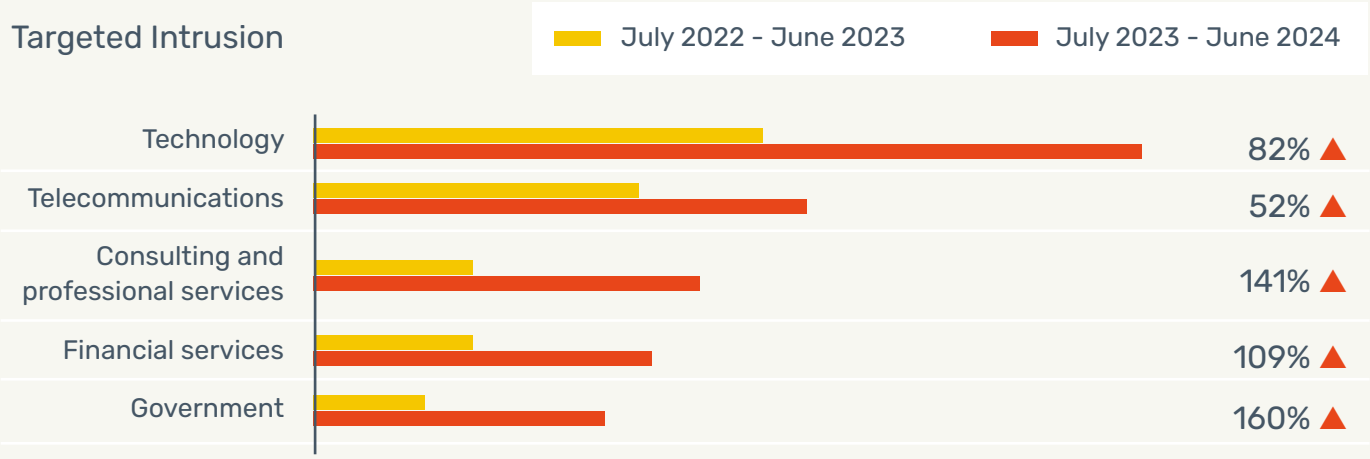
That year, Christine Lagarde, President of the European Central Bank and former head of the International Monetary Fund (IMF), warned that "a major cyber incident, if not properly contained, could seriously disrupt financial systems, including critical financial infrastructure, leading to broader financial stability implications."

In 2024, according to CrowdStrike's 2024 Threat Hunting Report,[6] financial services was in the top three categories of intrusion frequency for 2024, showing a 25% increase in intrusion events over 2023.



4 Ibid
5 "Modern Bank Heists' Threat Report from VMware Carbon Black Finds Dramatic Increase in Cyberattacks Against Financial Institutions Amid COVID-19, May 14, 202, Broadcom, https://news.broadcom.com/releases/modern-bank-heists-threat-report-from-vmware-carbon-black-finds-dramatic-increase-in-cyberattacks-against-financial-institutions-amid-covid-19
6 Crowdstrike 2024 Threat Hunting Report https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrike2024ThreatHuntingReport.pdf?version=0

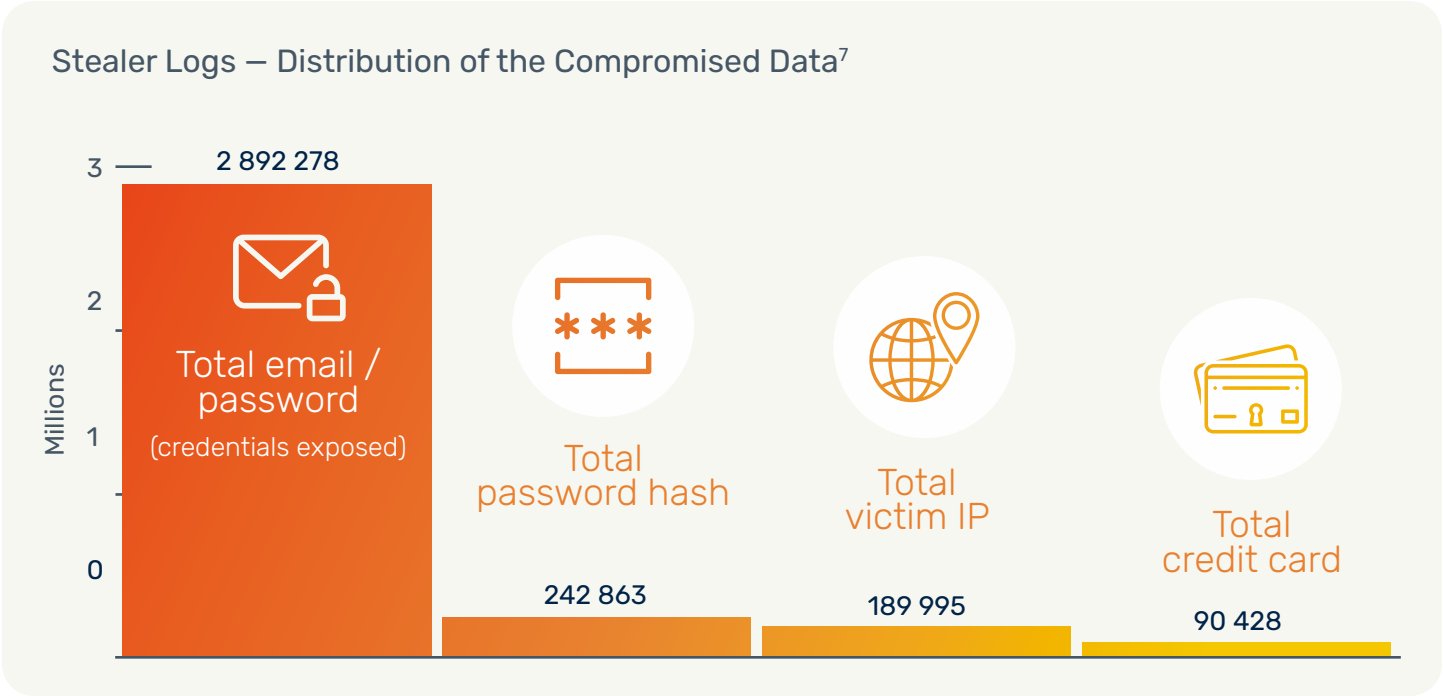
In the same time period, the number of intrusions directed to specific financial systems and institutions (as opposed to mass cyberattacks) increased by 109%.



The Adversaries are Gaining the Advantage

A fundamental shift is underway in the nature of threats to the financial sector. While phishing and business email compromise (BEC) remain primary initial vectors for bad actors, both are being supercharged by AI, as tools for impersonation, extortion and evasion tactics are leveraged for attacks. The generation of malware, deepfake videos, phishing websites and synthetic voices are being automated by tools including FraudGPT, BlackmailerV3, and ElevenLabs, resulting in more scalable, believable and effective campaigns.

What the phishers and impersonators are looking for is also shifting. SOCRadar's 2025 analysis of activity related to the financial sector on the dark web tracks the use of hacker forums and other platforms where stolen access to financial networks, tools, and data are bought and sold. Their analysis of more than three million posts found that the sale of valid credentials has far outpaced the sale of stolen credit card details:



Similar reports have found an explosion in the underground economy for stolen credentials and direct corporate access. There could be numerous reasons for the widening gap between the increase in credential logs and the increase in compromised credentials for sale. A credit card represents one account. An average person will have five to 10 bank accounts; as many reuse usernames and passwords, credentials could potentially access them all, plus social media accounts and more. Use of endpoints such as credit card numbers are heavily scrutinized by security processes, while use of valid credentials can allow threat actors to enter the system with minimum visibility and once there, avoid detection. Adversaries entering with valid credentials are able to "live off the land," using built-in systems and trusted applications to carry out malicious activities instead of introducing their own malware, which in an environment as protected as a bank, could easily set off alarms. Using existing credentials allows the hacker to maintain a low profile, extending their presence and elevating their permissions within a network, often without raising red flags.[8]

7 "Finance Industry Threat Landscape Report," February, 2025, SOCRadar, https://socradar.io/wp-content/uploads/2025/02/Finance-Industry-Threat-Landscape-Report.pdf
8 "2024 Threat hunting Report," Crowdstrike, n.d., https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrike2024ThreatHuntingReport.pdf

Stolen data had additional financial value for weaponization and use in the double and triple extortion rising in the threat landscape. In the past, ransomware primarily used a single extortion vector, encrypting data, freezing or bringing down systems in the process, and providing a decryption key on payment of the ransom. Today, adding data exfiltration to the attack allows for double extortion, extorting additional payments to not leak the data, while pressuring victims through customers, partners or regulators. In quadruple extortion, a relatively new development, threat actors escalate attacks by launching multiple cyber or physical attacks if demands are not met.

Stolen credentials and other sensitive data have proven to be so valuable that in some cases, threat actors have phased out encryption altogether. According to CheckPoint's *The State of Cyber Security 2025* report,[9] "by 2024, established groups like BianLian, a Russian-speaking ransomware group, fully transitioned to DXF-only extortion and abandoned encryption altogether. Similarly, Meow, an older ransomware group previously engaged in double extortion, re-emerged this year, focusing solely on data sales, offering stolen data at different price points, and allowing victims to "buy back" their information to prevent public exposure."

The shift has been facilitated by advances in 2024 in infostealers, malware designed to infiltrate systems and steal sensitive information, including credentials, financial data, session cookies and personal data, while working in the background without the victim's (or the cybersecurity team's) knowledge, then forwarding the data to the attacker's servers. According to CheckPoint, there was a 58% increase in infostealer infection attempts in 2024. Sixty-eight percent of infostealer attacks originated from email in 2024, most commonly in html attachments. Spoofed web pages and malicious sites are the second most common vehicle, followed by "password spraying," which employs several commonly used weak passwords (e.g. "Password123," or "admin") across large numbers of accounts, hoping that one unlocks a valid account. One of the main uses of password spraying is to extract credentials for accessing corporate systems on BYOD (Bring Your Own Device) equipment; over 70% of devices infected by infostealers are personal rather than corporate or managed.

Destruction of data as a part of a cyberattack, another means of "upping the ante" on ransom payment, is also on the rise. In 2024, over half (54%) of global financial institutions experienced cyberattacks in which data was destroyed by adversaries, including deleting data, destroying hard drives, terminating connections and executing malicious code to hide their tracks. In 2024, data destruction increased by 12.5% over 2023.[10]

9 "The State of Cyber Security 2025," https://engage.checkpoint.com/security-report-2025
10 Muncaster, Phil, "Destructive Attacks on Financial Institutions Surge," Infosecurity Magazine, February 5, 2025, https://www.infosecurity-magazine.com/news/destructive-attacks-banks-surge-13

The Global Picture

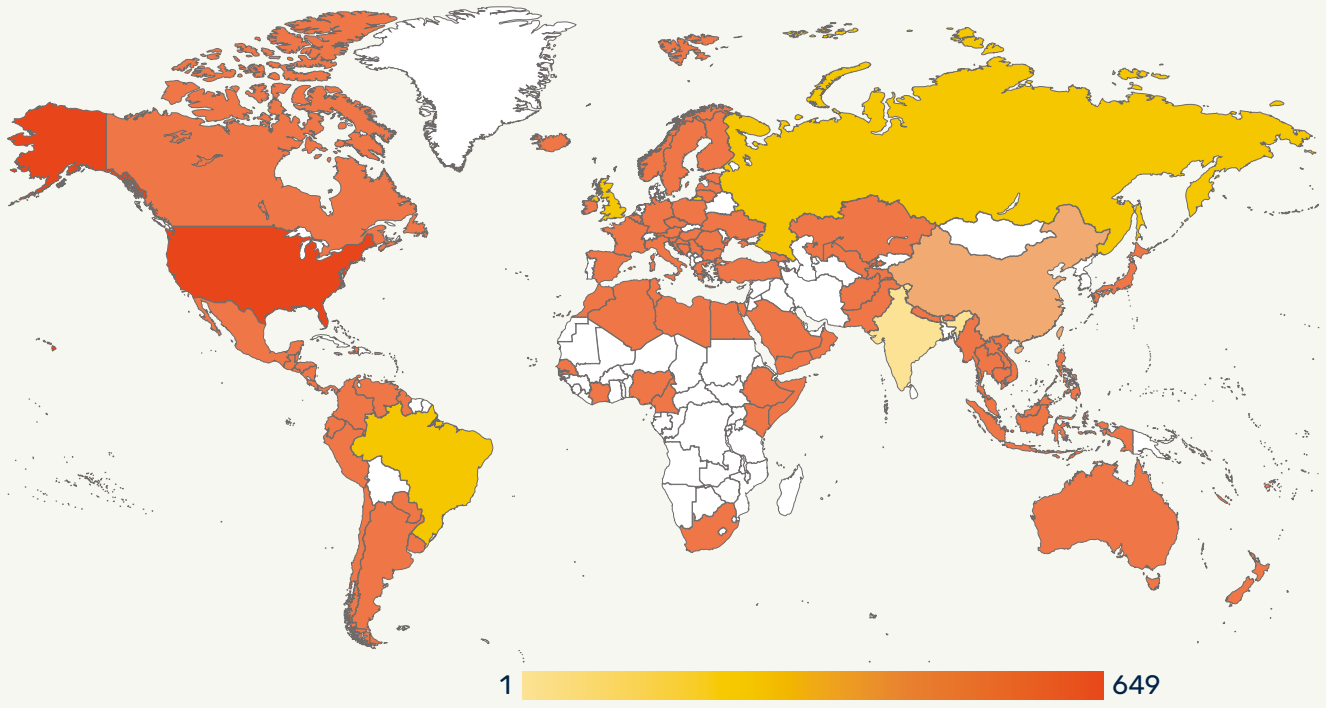
The United States financial sector, by far the most exposed to cyber threat, had the strongest surge in 2024, and the highest overall malicious cyber activities (19.10%). It was the primary target for both ransomware attacks (60.47%) and infostealer campaigns (18.81%).[12]

Emerging markets, particularly in South Asia and Latin America, are experiencing increased targeting by infostealers, suggesting that threat actors are also drawn to regions with expanding digital banking adoption and possibly weaker security controls.

Attacks are growing against Brazil, India and Pakistan, which are also areas with growing digital banking adoption coupled with less mature security culture. The rising threat in regions with high cryptocurrency adoption rates could indicate a rising interest in targeting populations that are seeking alternative financial services.

Narrowing the view to ransomware attacks alone, the dominance of the United States as a target is even higher, at 60.47% of all attacks. The United States and U.K. together account for 70.94% of all ransomware attacks, suggesting that ransomware groups are predominantly focused on English-speaking countries with developed financial markets. In the APAC region, Indonesia (5.81%), India (4.65%), China (2.33%), and Japan (1.16%) have been strategically targeted, but at much lower rates than Western targets.[13]

Targeted Countries for the Finance Industry[11]



11 "Major Cyber Attacks Targeting Finance Industry," SOCRadar, March 13, 2025, https://socradar.io/major-cyber-attacks-targeting-the-finance-industry/
12 Ibid
13 Ibid

Third- and Fourth-Party Attacks

Financial institutions are increasingly reliant on third-party vendors for core functions; fintech companies have become vital elements of the ecosystem, powering payments, compliance, fraud detection, and more. The rapid integration of outside systems has created new levels of interdependency, and new vulnerabilities, allowing a breach to a single vendor to impact companies across the entire system.

This is best illustrated by a December 2024 report by SecurityScorecard,[14] which found that 97% of the largest U.S. banks reported third-party breaches in 2024, though only 6% of vendors were compromised. Nearly all of the banks canvassed for the report also suffered fourth-party breaches, traced back to just 2% of vendors. A separate report from the same company found that 100% of Europe's biggest financial services companies had suffered a breach via their suppliers in 2024.[15]

Claims data released in April 2025 by cyber insurance firm At-Bay[16] found that financial fraud — most often following a phishing attack — remained the most common type of cyberattack leading to an insurance claim. The most damaging type of attack continued to be direct ransomware, but indirect ransomware — that is, exposure to ransomware through a third party — has "taken off," leading to rapidly rising risk for companies and their insurers. The At-Bay report notes that one of the advantages of entering a system through a third party is, as we have seen in other trends, the ability to operate undetected. Along with access to valid credentials for the system, compromise of a third or fourth party "allows an attacker to gain valuable context information, enabling them to break into an email chain or reference an outstanding invoice and basically craft a more believable, authentic message."

14 "SecurityScorecard Threat Intel Report: 97% of Leading U.S. Banks Impacted by Third-Party Data Breaches in 2024," December 12, 2024, https://securityscorecard.com/company/press/securityscorecard-threat-intel-report-97-of-leading-u-s-banks-impacted-by-third-party-data-breaches-in-2024/
15 Muncaster, Phil, "All Major European Financial Firms Suffer Supplier Breaches, December 17, 2024, Infosecurity Magazine, https://www.infosecurity-magazine.com/news/all-europes-top-financial-firms/
16 Lemos, Robert, "Financial Fraud, With a Third-Party Twist, Dominates Cyber Claims," April 11, 2025, Dark Reading, https://www.darkreading.com/threat-intelligence/financial-fraud-third-party-cyber-claims

Managing the Risk

Planting an infostealer, encrypting a system with malware, or exfiltrating data for sale, all have a common initial vector: someone had to be convinced to take an action, to click on something, download a file, or otherwise open the door that lets bad actors in. Someone had to open the attachment that had infected html in it. Or they clicked on the link that looked like their account page at their bank, and used their credentials to log into a fake page. Exploiting the risk of human error is what opens the first door.

Protecting the company and protecting the end user from exposure of data they have entrusted to the company, requires not only knowing the holes the threat actors will try to come through, but empowering the people in the organization who are potential entry points to close the door when they try. It requires managing human risk.

Effective security awareness training is the foundation of human risk management. Training employees to identify threats, to recognize phishing attempts and social engineering tactics, building their knowledge of security best practices and protocols, and integrating practice at spotting suspicious activity in realistic scenarios, has proven to be one of the most powerful and cost-effective first actions to reduce human risk and protect both the company's systems and the users' valuable personal data.

Each year, KnowBe4 analyzes the online behavior of users to determine a baseline of how many individuals, without security awareness training, are susceptible to clicking on fraudulent links in phishing emails. For its 2025 Phishing by Industry Benchmarking report, KnowBe4 analyzed the behavior of 14.5 million users across various industries and sizes. Tests are conducted without prior alerts, targeting individuals performing their routine work tasks without any specialized training. The resulting baseline statistics indicate a "Phish-prone Percentage™" (PPP) of 33.1% of users; in

Notable Data Breaches in Financial Sector, 2023 - 2025

LATITUDE FINANCIAL, AUSTRALIA (Financial services)

When: March 2023 | **How many records:** 14 million

What was exposed: Names, addresses, dates of birth, credit card details, driver's license numbers, passport numbers, and financial statements.

BANK SYARIAH, INDONESIA

When: May 2023 | **How many records:** 15 million

What was exposed: Not released

TRUIST BANK, USA

When: October 2023 (announced June 2024)

How many records: 167,000 +

What was exposed: work email addresses, account balances, dates of birth, job titles, names, partial credit card data, and phone numbers of Truist Bank employees, plus included 65,000 employee records from IBM TRIRIGA, 22,900 records from Azure Active Directory (AAD), and bank transactions containing names, account numbers, balances, and IVR funds transfer source code.

MR. COOPER, USA
(Largest non-bank mortgage servicer in U.S.)

When: October 2023 | **How many records:** 14.7 million

What was exposed: Names, addresses, phone numbers, Social Security numbers, dates of birth, and bank account numbers. The incident caused a November technical outage that impacted customer payments.

TIPALTI, USA (Financial technology)

When: December 2023 | **How many records:** Not released

What was exposed: Not released. 256 GB of "sensitive data" stolen, with confidential information that could be used for extortion.

LOAN DEPOT, USA (Mortgage and loans)

When: January 2024 | **How many records:** 16.6 million

What was exposed: Names, birth dates, social security numbers, email and postal addresses, financial account numbers, and phone numbers. Some systems taken off line.

other words, one out of three computer users tested were likely to click on a bad link in a phishing email. It then breaks the survey into industries and sectors, and divides these in turn by size of the organization.

In 2025, the initial baseline for the financial services industry was troubling. In the category of large companies, i.e. those with 1000-9999 employees, financial services had an initial baseline of 38.4%, and extra-large (more than 10,000) coming in at a staggering 44.7%. In other words, tests in large financial institutions found that more than four out of 10 employees were likely to click on a malicious link or download an infected file.

Small and medium sized organizations had lower initial PPP ratings — 23.1% for operations with 1-249 employees, 28.9% for 250-999 employees. These are slightly lower than the global averages, but still show that roughly one third of employees present substantial risk to the organization.

The good news is that consistent and comprehensive cybersecurity awareness training works. According to the study, 90 days into an integrated approach of educational content and simulated phishing tests changed the outcomes noticeably, with the Phish-prone Percentage in financial services organizations dropping to 18.8% in small organizations, 19.5% in medium sized organizations, and 19.8% in organizations with more than 1,000 employees.

After one year of cybersecurity awareness training, the Phish-prone Percentage dropped even more significantly; for small organizations it dropped to 3.1%, for medium sized organizations, 3.8%, and for large organizations, 4.8%.

With security awareness training as a foundation, KnowBe4 works to build and strengthen a security culture within the company, providing reporting tools, creating a supportive culture that encourages questions and interchange on vital security issues, and building a holistic, user-centric approach to comprehensive protection.

Notable Data Breaches in Financial Sector, 2023 - 2025

CROSS SWITCH, MALTA (Online payment gateway)

When: January 2024 | **How many records:** 3.6 million

What was exposed: Names, usernames, phone numbers, banking details, emails, locations, and dates of birth.

TMX GROUP, CANADA
(Including subsidiaries TitleMax, TitleBucks, InstaLoan)

When: February 2024 | **How many records:** 4.8 million

What was exposed: Name, dates of birth, passport numbers, driver's license numbers, federal and state identification card numbers, tax identification numbers, Social Security numbers, financial account details, phone numbers, physical addresses, and email addresses.

PRUDENTIAL FINANCIAL, USA

When: February 2024 | **How many records:** 2.5 million

What was exposed: Names and driver's license numbers.

HSBC AND BARCLAYS BANKS, UK

When: April 2024 | **How many records:** 512,000

What was exposed: Notary requests, security certificates, PIX keys, JKS files, security signing keys, compiled .jar files, source code stolen from GitLab, and other unsorted documents.

PATELCO CREDIT UNION, USA

When: June 2024 | **How many records:** 500,000

What was exposed: Names, Social Security numbers, driver's license numbers, dates of birth and email addresses.

EVOLVE BANK & TRUST, USA

When: July 2024 | **How many records:** 7.6 million

What was exposed: Names, Social Security numbers, bank account numbers, and contact details.

BANK SEPAH, IRAN

When: March 2025 | **How many records:** 42 million

What was exposed: Account numbers, passwords, and transaction histories.

DBS GROUP, SINGAPORE

When: April 2025 | **How many records:** 11,200

What was exposed: Names, addresses, and loan account numbers.

About KnowBe4

As the provider of the world's largest security awareness training and simulated phishing platform, 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 developed by an internationally recognized cybersecurity specialist.

Join more than 70k international organizations in trusting the KnowBe4 platform to strengthen your security culture and reduce human risk.

For more information, please visit **www.KnowBe4.com**

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

KnowBe4

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