knowbe4

November 2025

Cyber Risk in Finance and Banking Across EMEA

How emerging technologies and rising threats are redefining risk in the EMEA finance and banking sector

What's Inside

Risk in Banking and Finance

From mobile banking and cloud services to AI automation and cryptocurrencies, European, African and Middle Eastern banks are embracing technology at pace, reshaping operations, customer engagement and competitive positioning. But every new innovation expands the attack surface, giving cybercriminals, hacktivists and even nation-states new pathways to exploit.

There's no question that the finance and banking sector is a lucrative and data-rich target for cybercriminals. It comes as little surprise, then, that it is the second most targeted industry for cyberattacks across Europe, accounting for 18% of incidents in key industries.[1] The outcome? Regulatory repercussions, operational downtime and reputational ruin, all of which comes at the average cost of $5.56 million USD (currently €4.77 million EUR) per incident in 2025.[2]

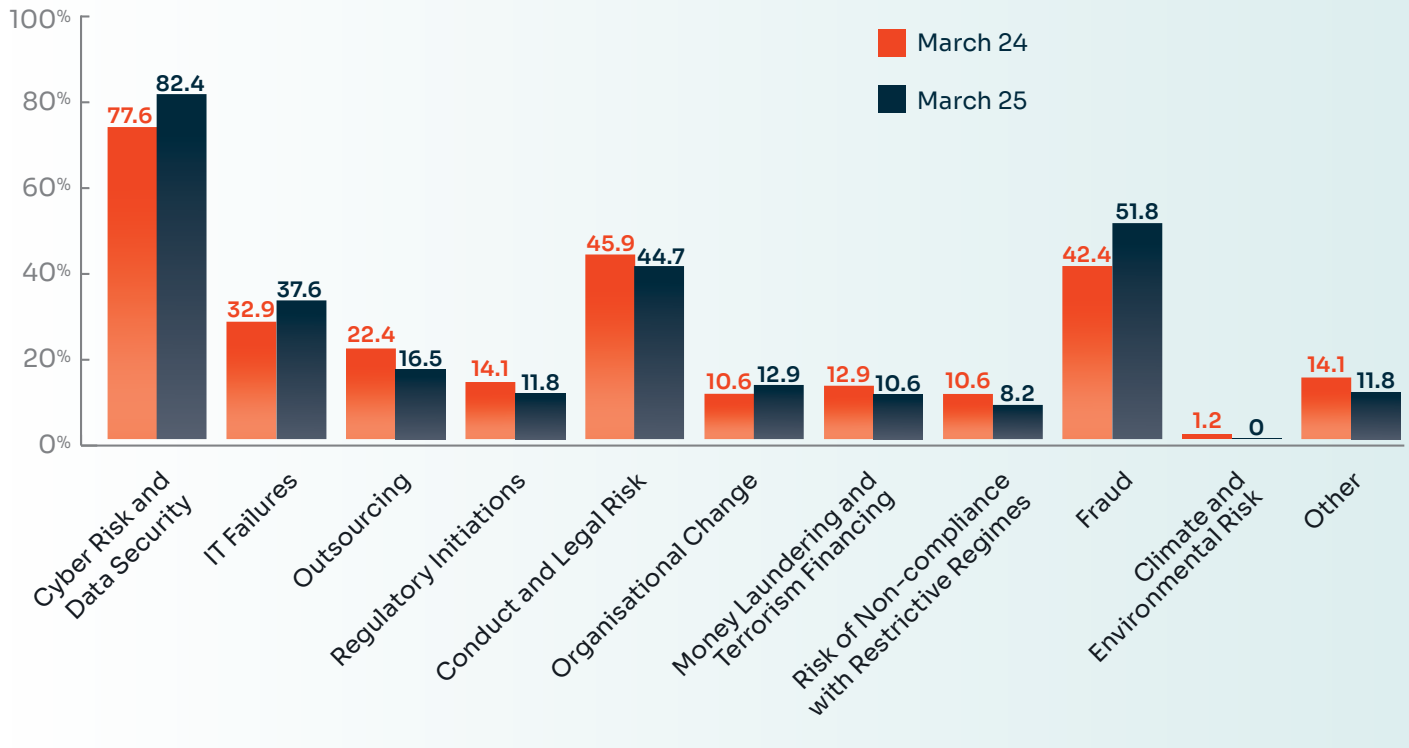
Set against a backdrop of rising regulations and rapid digital innovation, financial institutions are beginning to recognise cyber risk as a core strategic priority, competing alongside other business objectives rather than a back-office concern.

While it is clear that financial institutions are waking up to the harsh reality that cyber risk is no longer just an IT issue but a strategic business priority, the challenge is far from solved. Staying ahead requires more than investment in technology alone, but a holistic approach that also combines people, processes and governance to build resilience across the entire organisation.

Finance and banking is the second most targeted industry for cyberattacks across Europe.

Africa and the Middle East experienced the highest number of incidents in the finance and insurance sector, accounting for 27% of all cases. This indicates a growing financial landscape in emerging markets and a vulnerability in their cybersecurity defences that attackers are exploiting.[3]

Main Drivers of Operational Risk for Banking Institutions in 2025[4]



Early Adopters: The Digital Transformation

Over the past decade, the finance and banking sector in Europe has undergone a profound digital transformation, reshaping how institutions operate and deliver services.

Many financial institutions are recognising that this rapid expansion is creating a significantly broader attack surface.

From the rapid adoption of mobile banking apps, to the emergence of cryptocurrencies and more recently the integration of artificial intelligence (AI), financial institutions have consistently been early adopters of emerging technologies. While efficiency, customer-centric innovation, and scalability are key drivers of this shift, competitive pressure has also played a significant role. In a recent survey, over half of financial-services respondents (57%) reportedly admitted that they were concerned about 'keeping pace' with emerging technologies.[5] Another report found that 84% of financial institutions believe that failing to adopt AI and digitalisation in the coming years would negatively impact their business models.[6]

However, many financial institutions are recognising that this rapid expansion is creating a significantly broader attack surface, making the sector increasingly vulnerable to cyber threats.

In Europe, regulators have responded by strengthening the resilience requirements for financial services. The Revised Payment Services Directive (PSD2) mandated secure data sharing and enhanced customer authentication, paving the way for open banking while setting stricter security standards.[7] More recently, the Digital Operational Resilience Act (DORA) has introduced comprehensive rules for how financial institutions must test, manage, and oversee digital risks, including those arising from third-party service providers.[8] Together, these regulatory frameworks reflect Europe's recognition that digital transformation and cybersecurity must advance hand in hand to safeguard financial stability.

African countries lack continent-wide cybersecurity regulations for financial institutions, with most having their own national policies. For instance, South Africa has implemented a robust framework with the SARB's Directive in respect of Cybersecurity and Cyber-resilience within the National Payment System (NPS) 1 of 2024[9] and the Joint Standard 2 of 2024 on Cybersecurity and Cyber Resilience Requirements.[10] Nigeria's Central Bank implemented a Risk-Based Cybersecurity Framework and Guidelines[11] in 2024, mandating minimum cybersecurity requirements for banks. Ghana's financial institutions must comply with the Cybersecurity Act, 2020[12], and the Data Protection Act, 2012[13], with further directives from the Bank of Ghana. In Kenya, bank cybersecurity is primarily regulated by Central Bank of Kenya (CBK) guidelines[14], supplemented by the national Computer Misuse and Cybercrimes Act (2018)[15] and the Data Protection Act (2019)[16].

The United Arab Emirates (UAE) has a comprehensive regulatory framework for financial institutions and banks, primarily driven by the UAE Information Assurance (IA) Regulation[17], the Central Bank's Consumer Protection Regulation[18], and the Open Finance Regulation[19]. The IA Regulation focuses on cybersecurity, mandating robust security controls, risk management, and compliance measures to protect sensitive data and critical digital infrastructure.

The Consumer Protection Regulation ensures the safeguarding of consumer interests in financial products and services, promoting ethical conduct, transparency, and fair practices. Additionally, Article 13 on Technology Risk and Information Security[20] specifically outlines stringent requirements for Payment Service Providers regarding IT governance, cybersecurity risk management, user authentication, and business continuity. The Open Finance Regulation establishes a framework for secure data sharing and transaction initiation through an API Hub, imposing licensing requirements, capital adequacy, professional indemnity insurance, and strict data privacy and consent protocols for all participating licensees and Open Finance Providers.

The Saudi Central Bank (SAMA) has established a comprehensive Cyber Security Framework[21], mandatory for all regulated financial institutions in Saudi Arabia, including banks, insurance companies, financing companies, credit bureaus, and the financial market infrastructure. This framework, based on SAMA requirements and international standards like NIST, ISF, ISO, BASEL, and PCI, aims to standardize cyber security approaches, achieve appropriate maturity levels, and ensure proper risk management across all information assets. Additionally, the National Cybersecurity Authority (NCA) has issued Data Cybersecurity Controls (1:2022-DCC)[22] that mandate continuous compliance, self-assessment, and timely implementation by financial institutions. Specific implementation guidelines and timelines are also provided for the insurance and banking sectors, including detailed assessments, business plan development, and regular reporting to SAMA. Complementing these, the Personal Data Protection Law (PDPL)[23] establishes a legal framework for safeguarding personal data, outlining data subject rights and controller obligations, with key institutional support from the Saudi Data & AI Authority (SDAIA), the National Data Management Office (NDMO), and the NCA.

High Stakes, High Risks: The Cyber Appeal of the Financial Sector

The 2025 Verizon Data Breach Investigations Report (DBIR) said it best: the finance (and insurance) sector "has always had a large target painted on its proverbial back, given this is where the big money lives."[24] Financial gain is undoubtedly a primary motive for threat actors, but the sector's value extends beyond money, as sensitive personal and financial data are embedded in its core.

Cybercriminal groups exploit this through fraud, ransomware and data theft, capitalising on the potential immediacy of monetary rewards within banking systems. Nation-state actors view financial infrastructure as strategically significant, targeting it for espionage, disruption and leverage in geopolitical conflicts, with espionage motivated activity increasing in 2024 compared to the previous year.[25] Hacktivist groups occasionally enter the scene, aiming to undermine public trust or protest political and economic policies. Together, these diverse and persistent motivations make the finance and banking sector one of the most aggressively targeted industries in the global cyber threat landscape.

Understanding why financial institutions remain such a focal point for cybercrime requires the examination of the sector's defining characteristics:

Adoption of Digital Technologies

Emerging technologies are often initially unregulated, which can amplify risks when adopted early. As referenced, financial institutions are typically among the first to implement these innovations, but this early adoption also multiplies potential entry points for attackers. For example, McKinsey notes that increased cloud migration carries risks ranging from data privacy breaches to potential nation-state infiltration if not safeguarded with strong access controls and rigorous vulnerability management.[26]

Additionally, the combination of new technology with core legacy systems inherent in banking creates complex security gaps. The 'modernising around the core' approach taken by many banks (where new systems are layered onto old ones) reduces disruption but introduces integration issues and hidden vulnerabilities.[27] Ultimately this piecemeal system increases the risk of breaches, operational disruptions and regulatory non-compliance.

Third-Party Risk

As part of the digital transformation, many institutions are increasingly relying on third-party service providers, with IT outsourcing expenses rising by 7% and cloud expenses rising by 21% in 2023.[28] Whether that is cloud services, external partners, fintech collaborations or managed service providers, the interdependency exposes banks to risks beyond their direct control. The reliance on third parties blurs network boundaries, increasing the likelihood that attackers will exploit the weakest link in the supply chain. Without stringent third-party risk management, these vulnerabilities can cascade across multiple institutions, creating systemic weaknesses.

What's more, many major institutions tend to rely on the same/overlapping third-party providers, meaning a breach in one provider could cascade through a number of different institutions, amplifying the potential fall out.

High-Value Personal Data and Financial Assets

The concentration of high-value personal data and financial assets makes banks irresistible to cybercriminals. Financial institutions hold troves of sensitive information, from customer identities and transaction histories to market-sensitive corporate data. Unlike many other industries, the assets held by banks can be easily converted into financial gain, whether through fraudulent transfers, ransomware payments or data theft.

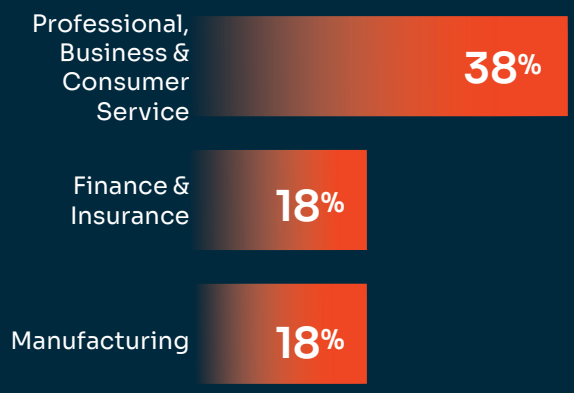
Critical Role in the Economy

Contrary to what is seen in many other sectors, these institutions play a critical role in national and global economies. Geopolitical tensions, which often aim to undermine economic stability, have heightened the cyber threat environment in Europe, with the European Banking Authority (EBA) warning of an increased likelihood of state-sponsored attacks on financial infrastructure.[29] Because financial systems are highly interconnected, even a single cyber event can disrupt global markets. Disruptions in this industry can halt clearing, trading and payments, undermining both financial stability and public trust.

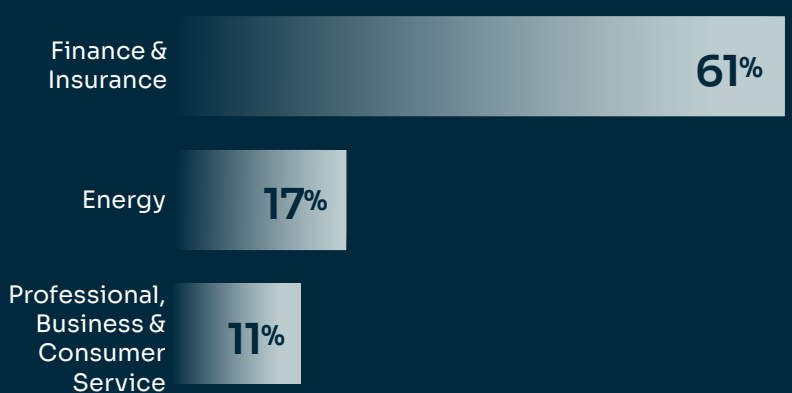
Rising Cyberattacks in Finance

Across Europe, the finance sector has recorded the second-highest number of cyber incidents, accounting for 18% of attacks on key industries in 2024, while the finance and insurance sector was the most attacked in the Middle East and Africa. Globally, this figure rises to 23%, making it one of the most consistently targeted sectors worldwide.[30]

Top 3 Industries Targeted by Cyberattacks in Europe in 2024[31]



Top 3 Industries Targeted by Cyberattacks in the Middle East and Africa in 2024[32]



According to a number of sources, threats against the sector are on the rise:

- In 2024, the ESRB observed that banks under the Single Supervisory Mechanism (SSM) reported the highest number of cyber incidents affecting credit institutions since data collection began.[33]
- In the EBA's Risk Assessment Questionnaire it was noted that 58% of banks had been victim to at least one cyberattack in the second half of 2024, compared to 55% in the first half of 2024 and the share of responding banks having faced at least one successful attack which resulted in an actual 'major ICT-related incident' increased 175% (12% to 33%) from September 2022 to March 2025.[34]
- According to the International Monetary Fund (IMF), nearly one-fifth of the reported cyber incidents in the past two decades have affected the financial sector, with banks being the most frequent targets followed by insurers and asset managers.[35]

The Real Impact of Rising Cyber Threats on the Financial Sector

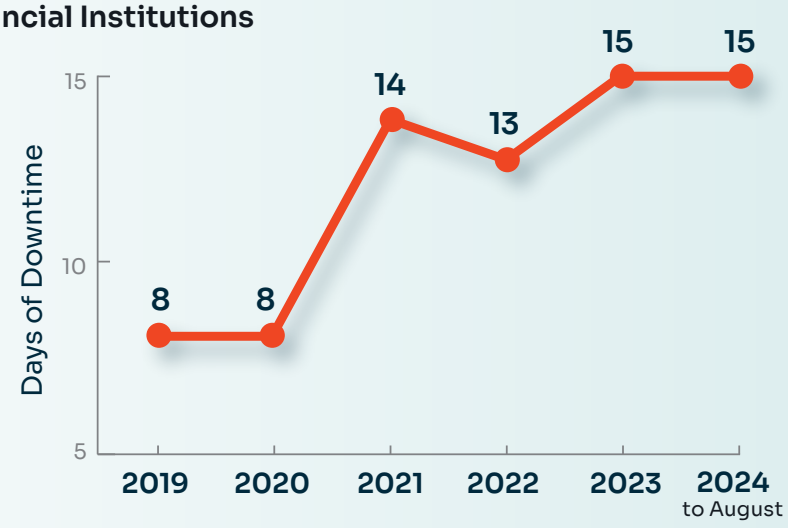
The consequences of this upward trend are potentially devastating for individuals, organisations and markets alike. For example, the finance and banking sector has consistently experienced some of the highest costs from data breaches. In 2025, the industry's average cost of a data breach stands at approximately $5.56 million USD (currently €4.77 million EUR), making it second only to the healthcare industry.[36] Cumulatively, financial institutions are estimated to have incurred losses of $2.5 billion USD worldwide (currently €2.4 billion EUR) since 2020.[37] Operational resilience is also at risk. Analysis shows that financial institutions experience an average of 15 days downtime following a ransomware incident, with some extreme cases lasting several months.[38]

In 2025, the industry's average cost of a data breach stands at approximately €4.77 million.

The United Kingdom's National Risk Register for 2025 even modeled a cyberattack on a UK retail bank as one of the largest threats facing the nation, highlighting that a reasonable worst-case scenario would see a bank's systems taken completely offline for several days, causing widespread service unavailability, fraud, and operational losses. Vulnerable customers would be most affected, and prolonged disruption could erode public confidence, potentially triggering customers to simultaneously withdraw their money leading to a liquidity crisis.[39]

At a systemic level, the International Monetary Fund's (IMF) Global Financial Stability Report stresses that cyber incidents in the financial sector represent a key operational risk with the potential to threaten macrofinancial stability.[40] Disruptions to clearing, payments or trading systems can undermine both confidence and economic continuity, with risks amplified by the global interconnectedness of financial markets.

Average Downtime for Analysed Financial Institutions following a Ransomware Attack[41]



How The Financial Sector is Being Targeted

Like other sectors across Europe, Africa and the Middle East, the finance and banking industry is facing a rise in both the frequency and sophistication of cyberattacks. While factors such as AI-assisted tactics are contributing to this trend, several primary attack methods appear to be driving many incidents in the sector.

Europe

Phishing and Spearphishing Attachments

Unsurprisingly, phishing continues to be one of the most effective methods for compromising financial institutions. According to IBM, attackers primarily breached finance and insurance systems through phishing and spearphishing emails containing malicious attachments, accounting for 30% of their analysed attacks from their 2025 report.[42] These attacks exploit human behaviour, relying on recipients to unknowingly open infected files or click on malicious links.

Spearphishing, a more targeted variant, is often aimed at specific individuals within an organisation, such as executives or employees with access to sensitive systems. By impersonating trusted contacts, attackers increase the likelihood of successful compromise.

Distributed Denial of Service Attacks (DDoS)

From January 2023 to June 2024, the ENISA Threat Landscape Report on the finance sector found that, of the threats analysed, DDoS attacks accounted for 46%, making them the most common type of attack in the data set.[43] A Distributed Denial of Service (DDoS) attack occurs when multiple systems flood a target such as a bank's website or online service with traffic, overwhelming its capacity and causing service disruption. Of the DDoS attacks observed, 58% targeted European credit institutions (banks), followed by government websites related to finance, tax and customs authorities at 21%.[44] The ECB also confirmed this trend, highlighting in their 2024 observations that DDoS attacks remained the most common type of incident.[45]

Ransomware Threats

Ransomware attacks have emerged as a particularly concerning threat for the financial sector, with the potential to disrupt widespread banking operations. The number of ransomware attacks on financial institutions and their service providers has surged, reflecting the growing sophistication and scale of these threats.[46] The financial impact of ransomware is especially severe in this sector. According to recent analysis, ransom demands targeting global financial institutions are among the highest of any industry, with average ransom demands of $4.2 million USD (currently €3.6 million EUR) and average ransoms paid at $7.4 million USD (currently €6.3 million EUR)[47].

Third-Party and Supply Chain Risk

As financial institutions increasingly rely on third-party service providers, supply chain risk has become a major concern. Third-party management remains a key issue, with 65% of financial services respondents in a recent survey highlighting it as their greatest capability weakness.[48] Reliance on external providers for cloud computing, AI and other emerging technologies increases exposure to risks such as data breaches and system vulnerabilities which can be amplified when institutions have limited visibility and control over their providers' security practices. A weakness in one provider can cascade across multiple systems and institutions, potentially disrupting critical operations and undermining trust. Complex supply chains also make timely detection and response more difficult, allowing attackers to exploit vulnerabilities before they are addressed.

Recent research underscores the growing magnitude of these risks. Among Europe's top 100 financial institutions, 96% experienced a breach within their third-party ecosystem from March 2024 to March 2025, up from 78% the previous year. Geographically, the United Kingdom recorded the highest number of third-party breaches, followed by Germany and Switzerland.[49]

Africa[50]

Phishing

Online scams, particularly phishing, are Africa's most prevalent cyberthreat in 2024, significantly impacting individuals and organisations. Phishing accounts for 34% of all cyber incidents, with cybercriminals impersonating trusted entities via emails, messaging platforms, or fraudulent

websites to trick individuals into providing sensitive information. Tactics include AI-generated content, targeted social engineering attacks, mobile-based phishing (smishing), voice phishing (vishing), and social media phishing campaigns. These schemes affect critical sectors such as financial institutions, telecommunications, and government, emphasising the urgent need for robust, sector-specific mitigation strategies and enhanced forensic capabilities for African law enforcement agencies.

Ransomware

In 2024, ransomware emerged as a major cyber threat across Africa, with monthly detections increasing from the previous year and significantly impacting governments, businesses, and critical services. South Africa and Egypt experienced the highest number of incidents, followed by other digitised economies such as Nigeria, Kenya, the Gambia, Tunisia and Morocco. The financial repercussions were substantial, including outright theft, ransom demands ranging from thousands to millions of dollars, and significant recovery expenses. Critical infrastructure, such as Cameroon's electric utility and Kenya's Urban Roads Authority, faced disruptions, and government databases were compromised. Prominent hacker groups like LockBit, Hunters International, and BlackSuit employed methods such as double-extortion, data exfiltration before encryption, and public data leaks to target various sectors, leading to operational disruptions, data breaches, and threats to human health and safety.

Business Email Compromise (BEC)

BEC was identified as a significant and growing cyber threat, with a sharp rise in activity observed in 2024, particularly in West Africa. The finance sector was the most frequently targeted, affecting companies of all sizes. The sophistication of these attacks is increasing due to Cybercrime-as-a-Service (CaaS) and emerging AI-driven schemes, which utilise generative AI and deepfake technology to craft convincing emails and impersonate individuals, posing a significant risk by scaling attacks and enhancing their authenticity.

State of Cyberattacks Across Europe and Africa Over the Last Couple of Years

Germany

In 2023, Deutsche Bank suffered a significant data breach through its third-party account switching service provider, Majorel Germany. Attackers exploited a vulnerability in the MOVEit Transfer software used by the service provider, with the initial attack being linked to Russian-based Clop ransomware group. The breach exposed customer names and international bank account numbers (IBANs) for individuals who used the service between 2016 and 2020, though Deutsche Bank's internal systems were not compromised. According to some German media outlets other major German banks, including ING, Commerzbank, Postbank and Comdirect, were also affected due to the same use of the service provider.[51]

The website of Germany's Federal Financial Supervisory Authority (BaFin) experienced a DDoS attack in late 2023, making it partially inaccessible. At the time the Authority supervised 2,700 banks, 800 financial service institutions and over 700 insurance companies. Administrators quickly implemented security measures to protect operations and restore access. While the specific hacker group responsible remains unknown, financial institutions in Europe continue to experience increased pressure from similar DDoS incidents claimed by pro-Russian hacker groups.[52]

A cyberattack at the securities institution Traders Place, in June 2025, may have resulted in sensitive data falling into unauthorised hands. This data includes user numbers, first names, surnames, contact and address data, and securities account values as of November/December 2023. While Traders Place states that core and customer systems were not at risk and no misuse of data has been revealed, the German Federal Financial Supervisory Authority (BaFin), which supervises Traders Place confirmed the incident but could not provide further information due to confidentiality. The incident highlights the impact on financial institutions and their obligation to report serious ICT-related incidents under the DORA regulation.[53]

In late 2024, Nordea Bank was hit by an unprecedented wave of DDoS attacks.

United Kingdom

On New Year's Eve 2019, currency exchange firm Travelex suffered a Sodinokibi ransomware attack where cybercriminals exploited a vulnerability in the organisation's virtual private network (VPN) to gain unauthorised access and halt currency transactions. The hackers demanded approximately £5 million for stolen sensitive user data, and Travelex ultimately paid over £2 million in bitcoin. This attack led to four months of business interruption, an estimated loss of £25 million in the first quarter of 2020, and the organisation's eventual administration and restructuring. Travelex also faced penalties for failing to notify the ICO about the breach within 72 hours.[54]

Ireland

Blackpool Credit Union experienced a cyberattack in August 2025. This incident led to the potential compromise of personal data for approximately 6,500 members, including names, addresses, contact numbers, dates of birth, and credit union account information. While the main banking system and PINs were not affected, and no money was removed from accounts, there is a risk that this information could be disclosed on the dark web and used for financial scams or phishing attempts. The credit union has reported the incident to the Central Bank, the Data Protection Commission (DPC), and An Garda Síochána, and is directly contacting affected individuals. Members are advised to be vigilant against unsolicited or suspicious communications.[55]

Nordics

In late 2024, Nordea Bank was hit by an unprecedented wave of DDoS attacks.[56] The assaults severely disrupted its online platforms and highlighted the growing vulnerability of core banking services to sustained disruption campaigns. The scale and persistence of the attacks underscored the financial sector's exposure to cyber-activism and potential state-linked operations, prompting regional authorities and financial institutions to reassess resilience and defense measures.[57]

Finland

In 2022, the OP Financial Group of Finland experienced a cyberattack on its Osuuspankki website, leading to customers receiving phishing messages. Although the attack was averted and services restored, the incident highlights the importance of vigilant online banking practices, as a phishing attack can be the initial step for threat actors to breach a network.[58]

Netherlands

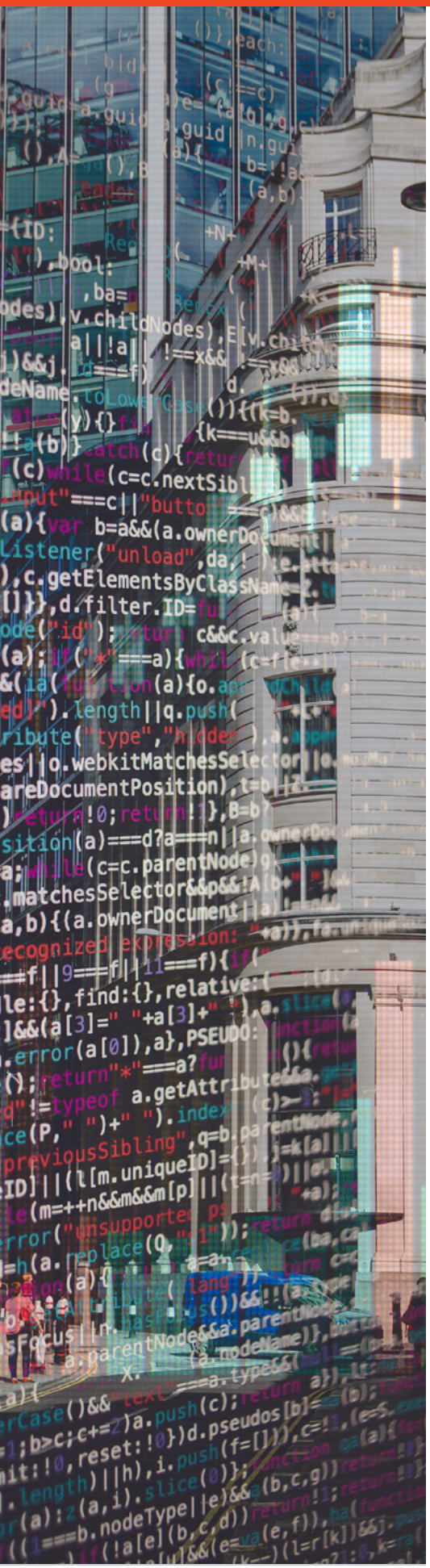
In 2023, Dutch banks including ABN Amro and ING were hit by a series of large-scale DDoS attacks that temporarily disrupted online banking and payment services such as iDeal, the country's dominant digital payment platform. Customers were left unable to access accounts or complete transactions, though no data loss was reported. The attacks highlighted how a coordinated assault on critical banking infrastructure could cause widespread disruption to everyday financial activity in the Netherlands, prompting renewed warnings from the Dutch Central Bank about the risks of cyber incidents spreading through interconnected payment systems.[59]

Belgium

In October 2024, hacking group NoName057 targeted banking services, the Federal Public Service for Economy, and the Belgian Centre for Cybersecurity (CCB) websites, in addition to the ports of Antwerp, Zeebrugge, Liège, and Brussels. These DDoS attacks overwhelmed servers, rendering some websites, like Febelfin, that represents the financial sector in Belgium, and the CCB, inaccessible for an extended period, significantly impacting the country's financial sector and cybersecurity infrastructure.[60]

Luxembourg

Local banks experienced "isolated interruptions" in services, such as online banking, during a Post cyberattack in July 2025, which caused a near-total breakdown of the telecom operator's internet and mobile services. While most financial institutions made a "rapid switch" to back-up systems, the incident led to temporary disruptions in internet connectivity, with some customers unable to access their bank accounts, and prompted several entities to plan strengthening their operational resilience.[61]



France

In early 2024, the French data protection agency, CNIL, launched an investigation into two data breaches at payment processors Viamedis and Almerys, affecting 33 million French citizens, nearly half of the country's population. This incident, which occurred five days apart for each company, is the largest-ever data breach for French citizens. Viamedis was compromised via a phishing attack on an employee, while Almerys was breached through a portal used by health professionals. The stolen data includes personally identifiable information (PII) such as marital status, dates of birth, national identification numbers, and health insurer names, though banking information, medical data, and contact details were not accessed. The CNIL has cautioned policyholders to be vigilant for follow-on social engineering attacks, highlighting that a single employee falling for a phishing attempt was a key factor in the breach.[62]

Africa

In an apparent failure of pressure tactics, the Medusa ransomware group published what it claimed to be Bank of Africa's data on February 11, 2023, after the bank refused to pay a ransom by its deadline. This incident highlights a rising trend of cyberattacks targeting financial institutions in Africa. These banks, often facing limited resources and less advanced cybersecurity infrastructure, are perceived as vulnerable, and the Bank of Africa, with its multinational operations and significant investment in digital technology, presents a large attack surface, increasing the potential impact of such breaches.[63]

South Africa

A cyber extortion gang, N4ughtySec, claimed in 2024 to have infiltrated most of South Africa's banks by breaching various credit bureaus. This followed previous attacks in March 2022, where N4ughtySecTU (an earlier iteration of the group) exfiltrated data from TransUnion and demanded a $15-million ransom, which TransUnion refused to pay. A year later, N4aughtySecGroup emerged, demanding $30-million each from TransUnion and Experian. In the latest incident, N4ughtySec did not make a financial demand but instead sought an apology and admission of security flaws from the institutions. As proof, they demonstrated access to current personal and financial data of two journalists.[64]

UAE

The UAE banking sector has been subjected to multiple cyberattacks, with Mysterious Team Bangladesh claiming responsibility for taking down the websites of Abu Dhabi Commercial Bank and National Bank of Fujairah in 2023. Anonymous Sudan previously launched DDoS attacks on First Abu Dhabi Bank and Mashreq Bank. These incidents, primarily executed through DDoS attacks, highlighted significant cybersecurity concerns in the region, exacerbated by 50,000 daily cyberattacks, prevalent email phishing, and substantial financial losses and data breaches for many organisations, underscoring the critical need for enhanced security measures.[65]

The Regulatory Pressure on Financial Cybersecurity in Europe and Africa

In light of increasing attacks across Europe, new regulations are redefining how financial institutions manage and report cyber risk. The Digital Operational Resilience Act (DORA), which came into effect in January 2025, requires financial entities to demonstrate robust ICT risk management, regular resilience testing and stronger oversight of third-party providers.[66] The NIS2 Directive broadens obligations further, mandating incident reporting and board-level accountability across critical sectors, including finance, while raising expectations for supply-chain security.[67]

For financial institutions, these measures are driving:

- More open reporting of cyber incidents to regulators and information-sharing networks.
- Stricter accountability at executive and board level for resilience failures.
- Increased investment in resilience testing, awareness training and third-party risk monitoring.
- A cultural shift from compliance as a tick-box exercise to embedding cyber resilience as a strategic priority.

While these regulations are a step in the right direction, adoption is still uneven. PwC found that only 4% of surveyed financial entities have fully integrated DORA into their day-to-day operations, while 65% are still in early stages of assessment as of March 2025.[68] Equally, NIS2 readiness averages just 58% across industries as of August 5, 2025, with persistent gaps in supply-chain security, crisis management and incident response.[69]

This slow implementation begs the question: are financial institutions really concerned about cyber risk?

There is not one, continent-wide cybersecurity regulation for banks and financial institutions in Africa; rather, each country has its own laws and directives. For instance, in South Africa the South African Reserve Bank (SARB) has established a comprehensive regulatory framework through directives and Joint Standards, such as Directive No. 01 of 2024, Joint Standard 1 of 2023 (IT Governance and Risk Management), and Joint Standard 2 of 2024 (Cybersecurity and Cyber Resilience).[70] These regulations mandate stringent cybersecurity controls, strong IT governance, risk assessments, resilience frameworks, compliance with best practices, safeguarding critical infrastructure, and strict oversight for third-party service providers within the financial sector.

In light of increasing attacks across Europe and Africa, new regulations are redefining how financial institutions manage and report cyber risk.

In Ghana, the Cybersecurity Act, 2020 (Act 1038),[71] provides the regulatory framework for cybersecurity activities, including the designation of critical information infrastructure for the banking and financial sector. Furthermore, the Central Bank introduced the 2018 Cyber and Information Security Directive[72] to address cybercrime in the rapidly growing local digital financial services sector. This directive outlines protocols for routine and emergency scenarios, delegation of responsibilities, communication and cooperation, coordination with government authorities, reporting mechanisms, physical security for IT data centers, and assurance of data and network security, requiring Regulated Financial Institutions (RFIs) to comply.

Financial institutions in Kenya must adhere to the Computer Misuse and Cybercrime (Critical Information Infrastructure and Cybercrime Management) Regulations,[73] 2024, and the Data Protection Act.[74] The Central Bank of Kenya (CBK) has launched a Banking Sector Cybersecurity Operations Centre (BS-SOC) to monitor threats and coordinate incident response, requiring all regulated entities to report cybersecurity incidents within stipulated timelines and collaborate with the BS-SOC to enhance sector resilience.[75]

Does the Finance Sector Care about Rising Threats?

According to HSBC UK's chief executive, Ian Stuart, in early 2025, cybersecurity investment is top of the banking groups agenda, with hundreds of millions of pounds being invested in improving IT systems.[76] But is this a mutual feeling across Europe? Multiple sources suggest it is.

- **EBA Risk Assessment Questionnaire:** 82.4% of banks view cyber risk as a primary driver of operational risk, making it the top priority over other key concerns such as fraud and IT failures.[77]
- **EY/Institute of International Finance (IIF) Survey:** For the second consecutive year, cybersecurity is a top concern for European banking chief risk officers, with 73% reporting it as a top risk management issue.[78]
- **McKinsey/Institute of International Finance Report:** 86.5% of financial services respondents (32 out of 37) highlight cyberattacks as a top risk priority, with attacks exploiting third parties and supply chains identified as key concerns.[79]

It appears overwhelmingly clear that financial organisations are aware of the increasing issue, and, what's more, the 'critical underinvestment' in the area. Financial services are reported to spend an average of 13% of their IT budget on cybersecurity but this is 'fortunately' expected to increase in the next few years.[80]

What Can Organisations Do to Address the Challenge?

Cyberattacks on the financial sector are frequent, sophisticated and costly. As digitalisation and third-party reliance expand, financial institutions can no longer rely on reactive measures. Building long-term resilience requires an integrated strategy that addresses both technical vulnerabilities and human factors.

1. Embed Cybersecurity into Digital Transformation

Cyber risk must be embedded in all digital channels, including mobile banking, online platforms and AI-driven analytics:

- Implement cybersecurity-by-design for new banking apps, cloud services and data platforms.
- Conduct regular risk assessments across digital services and customer-facing applications.
- Align with DORA, NIS2, PSD2, and other relevant regulatory frameworks.

2. Strengthen Third-Party and Supply Chain Oversight

Financial institutions increasingly depend on external providers, creating systemic risk:

- Maintain rigorous vendor risk management programs for all third-party providers.
- Require security audits and resilience testing from critical suppliers.
- Include third parties in incident response planning and communication protocols.
- Share threat intelligence with trusted partners to anticipate emerging risks.

3. Address the Human Element

Many attacks exploit human behaviour, particularly through phishing, social engineering or misconfigured systems:

- Support employees by deploying intelligent anti-phishing systems to neutralise sophisticated attacks.
- Provide personalised, relevant and adaptive security awareness training based on individual roles and departments.
- Run simulated phishing campaigns to improve detection and response.
- Offer just-in-time nudges to correct risky behaviour in real-time.
- Invest in cybersecurity talent and leadership, creating clear career pathways in IT and risk functions.

4. Balance Technology and People

While increased IT investments are great at strengthening defenses against DDoS and other technical attacks, threats such as ransomware, phishing and third-party breaches require attention to human processes, culture and behaviour to ensure true operational resilience.

Mitigating Human Risk in the Finance and Banking Sector

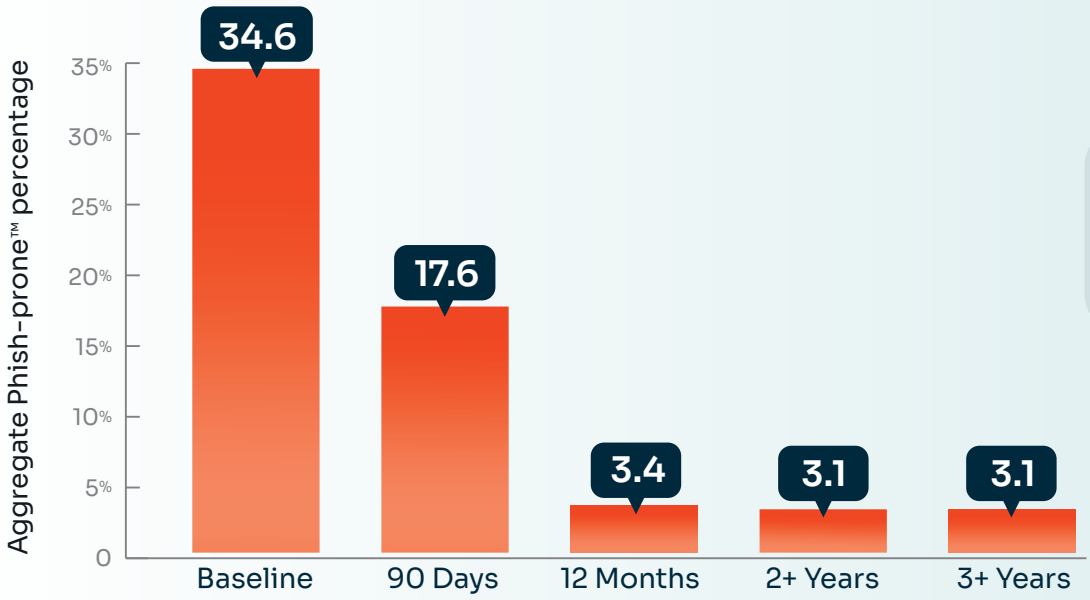
Each year, KnowBe4 measures an organisation's Phish-prone™ Percentage (PPP), the proportion of employees likely to fall for phishing or social engineering attacks. In the latest analysis of 67.7 million simulations across 14.5 million users in over 62,000 organisations, the European baseline PPP was 32.5%, meaning nearly one-third of employees interact with phishing simulations before taking part in best-practice security awareness training (SAT).

In the finance and banking sector, the baseline PPP across organisations of all sizes was close to the European average at 34.6%. However, after just three months of consistent and effective SAT, the overall PPP dropped significantly to 17.6%, demonstrating the powerful impact of SAT in reducing human risk. After 12 months, the PPP declined even further to just 3.4%, representing a 90% reduction. Encouragingly, this progress proved sustainable, with general click rates remaining low at 3.1% after two and three years consecutively.

With ransomware, phishing and third party risk playing a prominent role in cyberattacks targeting the finance and banking sector, it's clear that strengthening employee awareness and response is critical in building a stronger security culture, defending against initial access attempts and protecting the broader supply chain from compromise. By stopping attacks at the human entry point, organisations not only protect themselves but help prevent the spread of threats across the global economy.

The rise in cyber threats highlights that financial institutions must do more than just protect themselves; they must also defend the stability of the entire financial system. While increased investment in technology is paving the way for stronger defenses and faster threat detection, it is investment in people, their skills and their awareness and behaviour that ultimately determines an organisation's true resilience against cyberattacks.

Effective Training Lowers Phishing Click Rate in Finance and Banking Sector



90%
Reduction in Click-rate after 12 Months

1 "IBM X-Force 2025 Threat Intelligence Index," IBM.

2 "Cost of a Data Breach Report 2025" IBM.

3 IBM X-Force 2025 Threat Intelligence Index

4 "EBA Risk Assessment Questionnaire," European Banking Authority.

5 'The cyber clock is ticking: Derisking emerging technologies in financial services," McKinsey & Company

6 "Digital Operation Resilience Act, Laying the groundwork for digital resilience and transformation," PwC

7 Directive (EU) 2015/2366, OJ L 337 (2015)

8 Regulation (EU) 2022/2554, OJ L 333 (2022)

9 Directive in respect of cybersecurity and cyber-resilience within the national payment system, South African Reserve Bank

10 Financial Sector Regulation Act, 2017 - South African Reserve Bank and Financial Sector Conduct Authority

11 Overview of the CBN Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Banks

12 "Overview of the Cybersecurity Act 2020", Audrey Grey

13 Guidelines for Data Controllers/Processors on Compliance with the Data Protection Act 2012 (Act 843)

14 The Central Bank of Kenya, Banking Act (2015)

15 Computer Misuse and Cybercrimes, Kenya Law, The National Council for Law Reporting

16 Data Protection Act, 2019

17 UAE Information Assurance Regulation (1.1) Compliance

18 Consumer Protection Regulation, Central Bank of the UAE

19 Open Finance Regulation, Central Bank of the UAE

20 Article (13) Technology Risk and Information Security - Retail Payment Services and Card Schemes

Regulation - Central Bank of the UAE

21 Cyber Security Framework, Saudi Arabian Monetary Authority

22 Data Cybersecurity Controls. The National Cybersecurity Authority (NCA)

23 Personal Data Protection Law, Saudi Data & AI Authority

24 "2025 Data Breach Investigations Report," Verizon.

25 Ibid

26 'The cyber clock is ticking: Derisking emerging technologies in financial services," McKinsey & Company

27 "Modernizing legacy banking systems," Deloitte.

28 "IT and Cybersecurity Risk - key observations in 2024," ECB.

29 "Risk Assessment Report - June 2025," EBA.

30 "IBM X-Force 2025 Threat Intelligence Index," IBM.

31 Ibid

32 "IBM X-Force 2025 Threat Intelligence Index," IBM.

33 "Advancing macroprudential tools for cyber resilience - Operational policy tools April 2024," ESRB.

34 "Risk Assessment Report - June 2025," EBA.

35 "Global Financial Stability Report, April 2024" IMF.

36 "Cost of a Data Breach Report 2025" IBM.

37 "Global Financial Stability Report, April 2024" IMF.

38 "Financial organizations hit with average ransom demand of $4.2 million," Comparitech.

39 "National Risk Register 2025 Edition," HM Government.

40 "Global Financial Stability Report, April 2024" IMF.

41 Ibid

42 IBM X-Force 2025 Threat Intelligence Index," IBM.

43 "ENISA Threat Landscape: Finance Sector," European Union Agency for Cybersecurity.

44 Ibid

45 "IT and Cybersecurity Risk - key observations in 2024," ECB.

46 Ibid

47 "Financial organizations hit with average ransom demand of $4.2 million," Comparitech.

48 "The cyber clock is ticking: Derisking emerging technologies in financial services," McKinsey & Company

49 "Europe's Top 100 Financial Institutions Report," SecurityScorecard.

50 Interpol Africa Cyberthreat Assessment Report 2025

51 "Data leak also affects customers of the direct banks ING and Comdirect," Handelsblatt.

52 "German financial regulator's website hit by DDoS attack," The Record.

53 "Cyber incident at Tradersplace," Heise

54 "Travelex being held to ransom by hackers," BBC

55 "Blackpool Credit Union members' data may be on the dark web," Irish Examiner

56 "Nordea has come under "unprecedented" denial-of-service attacks," Helsinki Times

57 "Nordics move to deepen cyber security cooperation," ComputerWeekly.

58 "Finland's biggest bank reports cyberattack," Yle

59 "Renewed cyber attacks on Dutch banks ABN Amro, ING at weekend," DutchNews.

60 "Fourth consecutive day of cyberattack: Pro-Russian group takes revenge and shuts down the website of the Center for Cybersecurity," Nieuwsblad

61 "Luxembourg probes reported attack on Huawei tech that caused nationwide telecoms outage," The Record

62 "Data BreachesFrench Healthcare Payments Processor Breaches Affect Half of Population," Security Week

63 "Negotiation Fails, Medusa Ransomware Gang Leaks Bank of Africa Data," The Cyber Express

64 "Hackers claim they have access to South African citizens' financial data," Daily Investor

65 "Cyber Attack on UAE Banking Sector: Mysterious Team Bangladesh Claims to Hit First Abu Dhabi Bank," Cyber Express

66 Regulation (EU) 2022/2554, OJ L 333 (2022)

67 Directive (EU) 2022/2555, OJ L 333 (2022)

68 "Digitial Operation Resilience Act, Laying the groundwork for digital resilience and transformation," PwC

69 "Bridging the NIS2 Cyber Security Gap," Aon.

70 "SARB Cybersecurity and Cyber-Resilience Directive," Michalsons

71 "Banking Laws and Regulations 2025 – Ghana," Global Legal Insights

72 Bank of Ghana Cyber & Information Security Directive, Bank of Ghana

73 Computer Misuse and Cybercrimes, Kenya Law

74 Data Protection Act, 2019, Office of the Data Protection Commissioner

75 "CBK Launches Banking Sector Cybersecurity Operations Centre to Strengthen Financial Sector Defences," Tech Africa News

76 "Cyber-attack threat keeps me awake at night, bank boss says," BBC

77 "Risk Assessment Report - June 2025," EBA.

78 "Managing through persistent volatility: the evolving role of the CRO and the need for organizational agility," EY/IIF.

79 'The cyber clock is ticking: Derisking emerging technologies in financial services," McKinsey & Company

80 Ibid

About KnowBe4

KnowBe4 empowers workforces to make smarter security decisions every day. Trusted by over 70,000 organizations worldwide, KnowBe4 helps to strengthen security culture and manage human risk. KnowBe4 offers a comprehensive AI-driven “best-of-suite” platform for Human Risk Management, creating an adaptive defense layer that fortifies user behavior against the latest cybersecurity threats.

The HRM+ platform includes modules for awareness and compliance training, cloud email security, real-time coaching, crowdsourced anti-phishing, AI Defense Agents and more. As the only global security platform of its kind, KnowBe4 utilizes personalized and relevant cybersecurity protection content, tools and techniques to mobilize workforces to transform from the largest attack surface to an organization’s biggest asset. For more information, please visit www.KnowBe4.com

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