KnowBe4

Phishing, BEC, and Beyond:

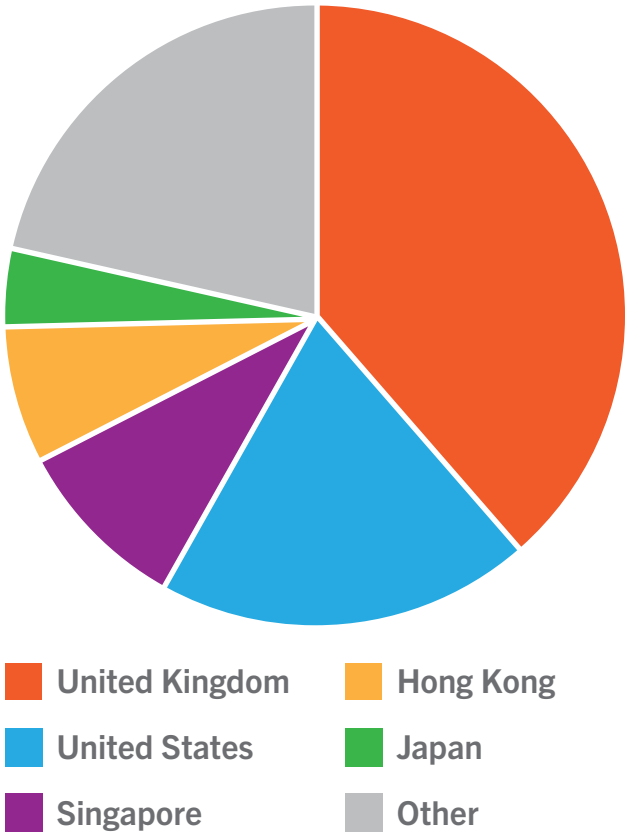
Tackling the Top Cyber Threats to UK Banks

THE BACKBONE OF THE BRITISH ECONOMY: THE FINANCIAL SECTOR

The United Kingdom's indelible footprint in the global financial sector is a source of national pride. A key driver of growth, the financial sector accounts for approximately 12% of the nation's GDP. It provides roughly 2.5 million jobs and pays more than £100 billion in annual taxes that provide crucial funding for public services.

From a global perspective, London is the leading Western centre for Islamic finance, offshore trading of the Chinese renminbi (RMB) and rupee denominated bonds. It is the world's leading international hub for debt issuance, commercial insurance, and currency trading, executing $3.8 trillion in daily forex transactions, more than one third of worldwide trades, and more than the next three largest centres – New York, Singapore, and Hong Kong – combined.

A key foundation to that international stature is trust, built in large part on an internationally recognised regulatory framework that provides stability to the sector. The potential cost of anything that could erode that trust is high.



Rising Cyber Threat

In 2021, Lyndon Nelson, deputy CEO and chief risk officer of Bank of England, addressed the risk of cyberattacks in a speech to a conference on financial markets and regulation. "For many," he said, "if cyber is not the number one risk in their risk register it is the fastest rising."[1] His words proved true by the last half of 2023, when the Bank of England reported that in its Systemic Risk Survey, for the first time, UK banks and other financial institutions cited the risk of cyberattacks and the resulting disruption of vital services as a higher and more alarming risk than geopolitical risks, inflation, or economic downturn. Ransomware was cited as one of the most acute threats, with other less sophisticated cybercrime following close behind.[2]

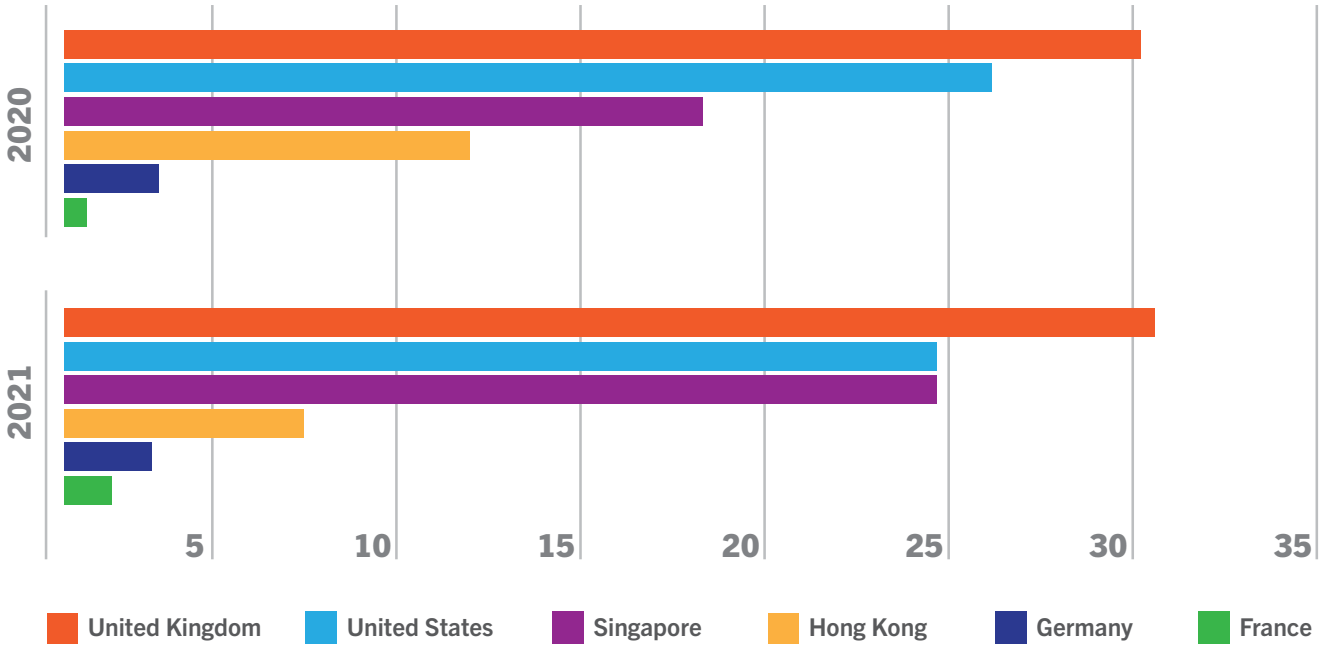
Not that geopolitics can be entirely divorced from cyber threats. In November 2023, the UK's National Cyber Security Centre warned of a rise of state-aligned groups and an increase in aggressive cyber activity, that the UK needs to accelerate work to keep pace with the changing threat, particularly in critical sectors including the financial sector. "Over the past 12 months," it said, "the NCSC has observed the emergence of a new class of cyber adversary in the form of state-aligned actors, who are often sympathetic to Russia's further invasion of Ukraine and are ideologically, rather than financially, motivated.

---

1 "Cyber Risk: 2015 to 2027 and the Penrose steps," Lyndon Nelson, 25 May 2021, https://www.bankofengland.co.uk/speech/2021/may/lyndon-nelson-the-8th-operational-resilience-and-cyber-security-summit

2 Systemic Risk Survey Results, 2023 H2, 10 October 2023, https://www.bankofengland.co.uk/systemic-risk-survey/2023/2023-h2

The UK remains the world's preferred regulatory regime for financial services



"In your view, which market currently has the most favourable regulatory regime for financial services?" % of interviewees

According to a 2023 report from Bridewell,[3] cyberattacks against financial service firms in the UK had surged a staggering 81% in the year following the Russian invasion of Ukraine – a far higher surge than the global increase of 61% in the same time period. Luke McNamara, deputy chief analyst at Mandiant Intelligence, Google Cloud's cybersecurity business, suggests that this surge of attacks from "espionage actors", including nation states, is related to the roles they play in "politically sensitive functions, such as sanctions enforcement and compliance, or financing of high-profile or controversial projects".[4]

Financial service organisations in the UK hold 20 percent more data than those in other sectors. This means a larger surface area to attack, and more potential blind spots for CISOs.

Tris Morgan, managing director of security at the UK telecoms group BT, also noted in January that "the financial sector is grappling with an escalating onslaught from cybercriminals." His company's data reveals, on average, "more than 46 mn signals of potential cyberattacks every day, worldwide" — with banking emerging as the most vulnerable industry.[5]

For an industry built on trust, the potential costs of cyberattacks can be staggering. Attacks on the financial sector can not only lead to financial loss and exposure of personal information, but disruption to the nation's financial infrastructure, and even threats to political stability "as confidence in financial markets is essential for global economic health".[6]

---

3 Cyber Security in Critical National Infrastructure Organizations, Financial Services. https://www.bridewell.com/insights/white-papers/detail/cyber-security-in-critical-national-infrastructure-organisations-financial-services

4 Ibid.

5 Murphy, Hannah, "Cyber attacks reveal fragility of financial markets," Financial Times, 16 January, 2024, https://www.ft.com/content/a8b8de58-8691-4ece-ade3-5b7be63dbef2

6 Ibid

Open Banking and Cyber Threats

In January 2018 the UK's Competition and Markets Authority (CMA) introduced Open Banking, a series of reforms, which with the CMA's new Payment Services Directive (PSD2), requires banks and other Financial Services and Insurance (FSI) businesses to allow third-party providers access to customers' banking data via application programming interfaces, or APIs. As a result, banking customers, both individuals and organisations, were able to use third party providers to access and manage their financial accounts and assets, transfer funds, and make payments via internet apps.

A boon for customers, online payment services, and online banks, the move created a dramatic shift in the security landscape for the sector. As the number of APIs has increased dramatically in the four years since the reforms were introduced, so has the volume of sensitive financial information being transferred at the data level; as can be expected, the shift has created new opportunities for malicious actors. According to some reports malicious software applications are responsible for more than a quarter (27%) of all traffic to British financial businesses. The industry is also being heavily targeted with Account Takeover (ATO) attempts, with roughly 40% of all ATOs hitting financial websites.[7]

Ransomware Attacks in Financial Sector Doubled in 2023

Britain's Financial Conduct Authority (FCA) regulates over 50,000 organisations operating in the nation's financial sector; firms are mandated to report all material cyber incidents to the regulatory body. A material incident is defined as a cyber incident that results in significant loss of data, or loss of control of its IT system, one that impacts a large number of victims, or one that results in unauthorised access to or malicious software present on its information and communication systems.

In January 2023, the FCA responded to a freedom of information act request by Picus Security with a report that they had received 51 cyber incident reports in the first half of 2023. While this represented only an 11% increase compared to the same period in 2022, the FCA was alerted to 19 ransomware incidents – a 200% increase over the same time period in 2021. Nearly one third (31%) of all cyber incidents reported were categorised as ransomware.[8]

The most widely reported of these was a ransomware attack that hit financial data firm ION Trading UK on 31 January 2023, that left scores of brokers unable to process derivatives trades. While the firm's parent company said in a statement the same day that "the incident is contained to a specific environment, all the affected servers are disconnected, and remediation of services is ongoing," the attack is a clear illustration of the potential far reaching effects from one attack to the sector.

In London, the Futures Industry Association (FIA) reported that the attack had affected the trading and clearing of exchange-traded financial derivatives, and that affected firms were using legacy systems and manual processing while ION's systems were out of operation.

Intesa Sanpaolo, Italy's largest bank, told clients that its brokerage and clearing operations on exchange-traded derivatives had been "severely hampered" by IT problems at ION and that it was unable to handle orders. On 1 February, a source familiar with the matter told Reuters that

---

7 Mascellino, Alessandro, "Financial Services Targeted in 28% of UK Cyber-Attacks Last Year," Infosecurity Magazine, 31 January 2023, https://www.infosecurity-magazine.com/news/quarter-cyber-attacks-uk-financial/

8 Picus Labs, "Ransomware Incidents Reported to UK Financial Regulator Doubled in 2023," 11 January 2024, https://www.picussecurity.com/resource/blog/ransomware-incidents-uk-financial-regulator-doubled-2023

"the attack put brokers that process complex over-the-counter trades involving products such as options in a difficult situation and the problem could take another five days to fix."

The U.S. Commodity Futures Trading Commission said that its weekly Commitments of Traders report would be delayed because of the attack, and that "certain reporting firms do not have enough information to fully prepare the daily large trader reports."

Chicago-based ABN AMRO Clearing, which operates from APAC and EU as well as the US, told clients the day after the attack that due to "technical disruption" from ION, "some applications were unavailable and were expected to remain so for 'a number of days."[9]

PREPARING FOR THE RISING THREATS

Deepfake audio, impersonation of a family member, CEO, etc. by an AI generated voice to deceive the receiver into transferring funds to cybercriminals, is emerging as a growing attack vector across the United Kingdom. But the "tried and true" phishing and BEC (Business Email Compromise) remain the top attack vectors against the business community.

One would think that this would be cause for fast action from the banking community, to protect banking customers and their accounts from fraudulent actors, and to raise awareness among users on how to spot a phishing email or text or a deepfake phone call. Encouragingly, in an April 2023 survey of 2,263 UK businesses,[10] in the category of finance and insurance, 75% of those surveyed said they consider cybersecurity a "very" high priority, compared to just 36% of all UK businesses. The same survey found that 79% of the organisations in the finance and insurance sector had sought external guidance and information on the cyber threats faced by their organisations in the previous year, compared with just 49% of the overall business community.

It is a question of whether the financial institutions can move quickly enough to meet the evolving threats. And despite a high level of confidence professed by banking leaders, the answer is not all good news.

There is a startling lack of basic security protocols to protect banking customers from either BEC or phishing. In February 2023 Red Maple Technologies released the results of research performed for consumer reporting company Which, having tested more than a dozen of the UK's largest banks across four areas of security, including login, navigation and logout, account management, and encryption for both online banking security and app security. The investigation found several banks missing basic online and app protections, including use of outdated and vulnerable web applications, failure to force secure passwords, not sending alerts when sensitive account changes including changes in email were made to accounts, and more.

EFFECTIVELY PROTECTING AGAINST CYBERATTACKS

The common denominator of nearly all cyberattacks is how the cybercriminal gains access to accounts or servers. Depending on the report you read, between 79 and 91% of all cyberattacks begin with a phishing email.

---

9 Person, James, and Masoni, Danilo, "Ransomware attack on data firm ION could take days to fix – sources," Reuter's, 3 February, 2023, https://www.reuters.com/technology/ransomware-attack-data-firm-ion-could-take-days-fix-sources-2023-02-02/

10 "Cyber security breaches survey 2023." Department for Science, Innovation, and Technology, 19 April 2023, https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023

Fortifying technical defences, including enforcing strong authentication as well as advanced threat detection systems, regularly patching software, and conducting security audits, will help to ensure malicious emails do not reach the employee who could fall for a fraudulent transfer or a user who could unwittingly give attackers access to his or her accounts. Collaboration and sharing of threat intelligence, not only among peer organisations, but through engagement with regulators, law enforcement, and cybersecurity experts, will strengthen the industry as a whole.

For the ones who still get through (and there will be some), the last line of defence, in many ways the most vital defence, is security awareness training to help staff and users recognise and report potential threats such as phishing emails or suspicious activity. Regular training and drills simulating phishing and BEC attacks not only prevent attackers from gaining access to accounts; they foster a vital culture of cybersecurity that resonates throughout the organisation.

As banking increasingly shifts toward fully digital operations, the need for that security culture has accelerated, becoming imperative to maintaining the foundation of the nation's finance sector – the level of trust and prestige it has earned in the international community.

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 UK, Ltd. | 1 Leeds City Office Park, Leeds, LS11 5BD | Tel: +44 (0) 1347 487512
www.KnowBe4.com | Email: Sales@KnowBe4.com

01E05K01