Cyber security in the UK financial industry

The threat landscape

Exploring the threat landscape

According to research from Verizon, the number one motive for cyber threat actors, by far, is **financial** – and it's been that way since 2015[1].

It's no surprise, then, that cybercriminals go after organisations that handle the money, with over a quarter of cyber attacks in the UK in 2022 being targeted at the financial services and insurance (FSI) industry[2].

This bleak threat landscape has not gone unnoticed by industry insiders. In 2022, the Bank of England polled 65 executives in the UK financial sector and found that 74% deemed a cyber attack to be the greatest risk faced by the sector in both the short- and long-term[3].

Financial services executives rated cyber attacks as a greater risk to the sector than inflation or a geopolitical incident[4].

So, what does the threat landscape look like for a financial services organisation in 2023?

Well, to understand this, it's important to understand the backdrop of Open Banking reform.

Let's jump straight in.

[1] Verizon Data Breach Investigations Report (DBIR), 2022. [2] InfoSecurity Magazine, 'Financial Services Targeted in 28% of UK Cyber-Attacks Last Year', 31 January 2023.
[3] Bank of England, Systemic Risk Survey Results – 2022 H2. [4] Bank of England, Systemic Risk Survey Results – 2022 H2

Open Banking

Is it open season for cybercrime?

In January 2018, the Competition and Markets Authority (CMA) introduced a series of reforms known as Open Banking, which emerged alongside the CMA's new Payment Services Directive (PSD2). The directive enables banking customers, whether they are individuals or organisations, to use authorised third-party providers to manage their finances.

So, for example, a consumer could use a third-party app to pay their bills, make transfers and analyse their spending, with the money still being secured in their bank account.

How does Open Banking work?

An example

A bank customer downloads a third-party automatic savings app.

The customer gives the app permission to access their banking data.

Their information is shared by the bank via an application programming interface (API).

The app analyses the account data to calculate a savings plan.

The app moves money into a savings account.

The problem with Open Banking, however, is that giving third parties access to customer accounts using open APIs opens up various cyber risks.

For consumers, these relate mainly to the increased risk of a data breach, but for financial institutions, it changed the whole threat landscape.

In the shadows

Open Banking significantly increased the number of APIs in use in the FSI industry, increasing the risk posed by **shadow APIs.**

These untracked APIs are completely unmonitored and vulnerable to being exploited by cybercriminals, who could manipulate them to:

- Access private user accounts
- Alter or delete user information
- Access sensitive information
- Change user credentials

The scale of unmonitored API traffic is substantially higher than in other industries, suggesting that FSI companies' implementation of Open Banking standards may have inadvertently created a serious, industry-wide security threat.

Andy Zollo, regional vice president for EMEA at Imperva[5]

Ransomware

While Open Banking changed the threat landscape for the FSI industry, it can't take the blame for all of its cyber security woes.

Ransomware is one of the biggest threats to the industry, which has seen numerous high-profile attacks in recent years.

74% of global financial institutions experienced at least one ransomware attack in 2021[6].

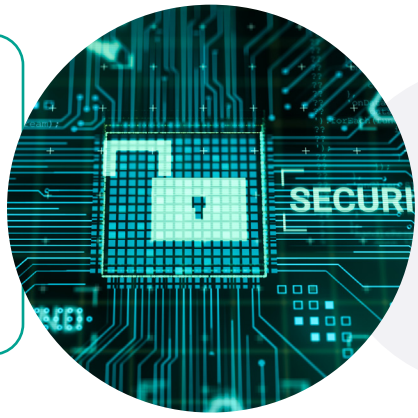
Ransomware attack causes chaos in City of London[7]
February 2023

City of London traders have experienced mayhem after software supplier Ion Group, which produces vital trading software, was the victim of a ransomware attack. The attack affected over 40 of Ion's clients, some of whom were forced to use pen and paper to process their trades.

Today, ransomware poses a bigger threat than ever to the industry, in part due to the rise of Ransomware-as-a-Service (RaaS), which has enabled cybercriminals to quickly and easily scale up their attacks.

AI and the future of cybercrime

RaaS is one thing, but artificial intelligence (AI) is fast becoming another tool cybercriminals can use to improve the success of their ransomware attacks. Expect to see AI-powered attacks increase in the years to come.



[5] InfoSecurity Magazine, 'Financial Services Targeted in 28% of UK Cyber-Attacks Last Year', 31 January 2023.

The human error element

The Verizon report shows that while 73% of FSI data breaches in 2022 were committed by external threat actors, the other 27% were internal[8], and this is where the human error element comes in.

What Verizon has termed 'Miscellaneous Errors' represented a high number of data breaches for the FSI industry in 2022. Often, these took the form of 'misdelivery', where PII or other sensitive information was sent to the wrong recipient.

As well as inadvertent data breaches, human error is commonly exploited by cybercriminals to commit attacks.

To gain access to victims' systems, for example, attackers may:

Send phishing emails

Brute force weak passwords

Exploit misconfigured web servers

Take advantage of unpatched devices

How TSC can help

At TSC, we are experts in security training and behavioural change. We can support you to address the threats you face in the current cyber security landscape, and help you reduce the human error risk.

If you would like more information about how The Security Company can help, please contact us via: **enquiries@thesecuritycompany.com** or call on **01234 708456**.

Cyber risk in the financial services sector:

don't let it co$t you.

www.thesecuritycompany.com **@TSCPeopleSec** **@thesecurityco** **@thesecurityco**

[6] Financial Times, 'The financial system is alarmingly vulnerable to cyber attack', 16 February 2023.
[7] Computer Weekly, 'Suspected LockBit ransomware attack causes havoc in City of London', 2 February 2023. [8] Verizon Data Breach Investigations Report (DBIR), 2022.