PICUS

CYBER SECURITY INCIDENTS IN

THE UK FINANCIAL SECTOR:

An Analysis of FOI Data Supplied by the FCA

1. Introduction

Financial services firms continue to be an extremely attractive target for cybercriminals. While on the whole, the sector is aware of the risks it faces and prioritises security accordingly, the latest techniques that cybercriminals use means that preventing and detecting attacks is increasingly challenging.

To obtain an up-to-date picture of the operational resilience of the financial industry in the UK, Picus Security submitted a Freedom of Information (FOI) request to the Financial Conduct Authority (FCA).

The FCA regulates the activity of more than 50,000 financial services firms in the UK and mandates that all firms under its jurisdiction must report 'material' cyber security incidents.

This report has been produced to analyse the total number and type of incident reports submitted to the FCA in 2021 and compare this data against similar information disclosed previously.

Contents

2. The State of Cyber Security in Finance

Key findings

- The FCA received 116 reports of 'material' cyber security incidents in 2021, up from 76 in 2020 (an increase of 52%).
- 65% of cyber incidents in 2021 (75) were due to cyber attacks.
- Approximately one third of incidents (37) contained notifications where the confidentiality of company or personal data may have been compromised or breached.
- One in five incidents reported to the FCA in 2021 involved ransomware.
- 21 cyber incidents were reported to the FCA in March 2021 – the most submitted in any month that year and coinciding the disclosure of critical vulnerabilities in Microsoft Exchange Server.

What is a material cyber security incident?

Should any financial services firm suffer a 'material cyber incident', it must notify the FCA. According to the FCA, an incident may be material if it:

- results in a significant loss of data
- results in the unavailability or control of IT systems
- affects a large number of customers
- results in unauthorised access to information systems

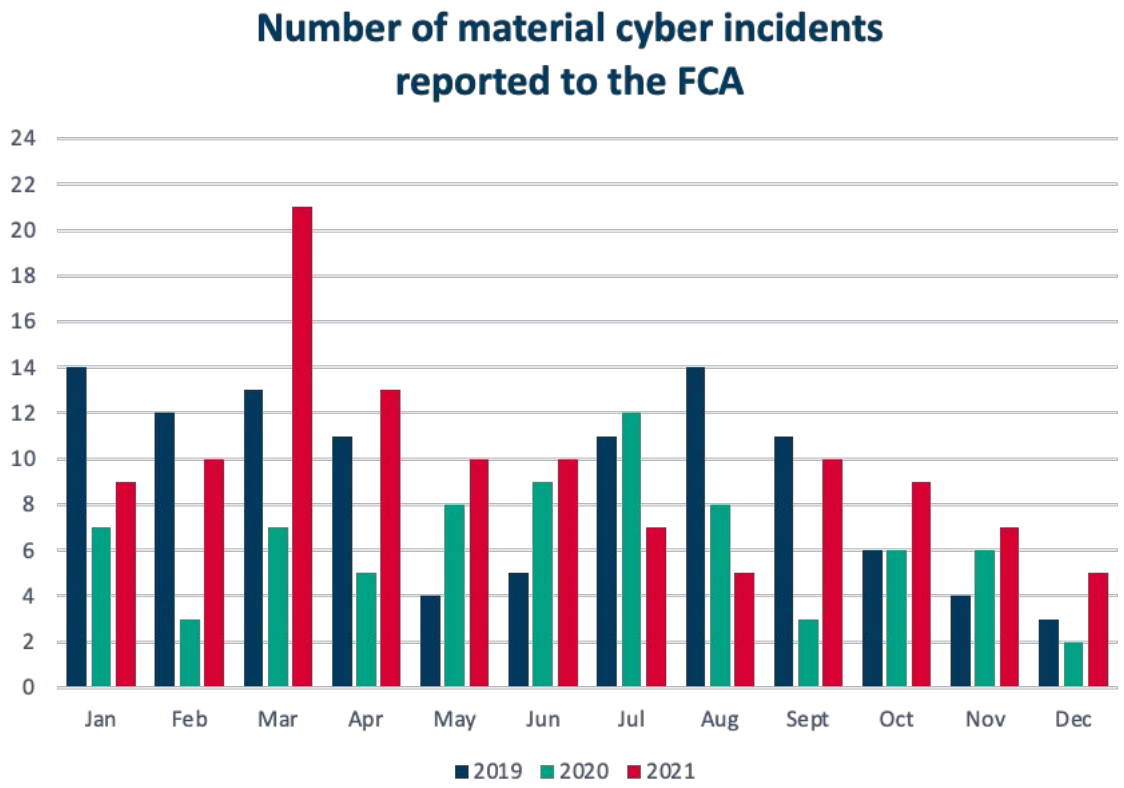
N.B. Depending upon the type of incident, a firm may also need to notify Action Fraud, The Information Commissioner's Office (ICO) and the National Cyber Security Centre (NCSC).

3. Reported Incidents on the Rise

The number of material cyber incidents reported to the FCA in a calendar year is a good measure of the resilience of financial sector firms.

In 2016, the FCA disclosed that it had received 90 material cyber incident reports*, a number that rose to 106 in 2019 before decreasing to 76 in 2020**.

In 2021, our FOI data shows the number increased by 52% to 116.



Of the total number of material cyber incidents reported to the FCA in 2021, we learned that 65% (75) were the result of cyber attacks. The remaining incidents are likely explained by system and process failures as well as employee errors.

Approximately one third of all cyber incidents (37) involved a data breach, where data was lost or stolen.

* Source: www.fca.org.uk
** Source: www.kroll.com

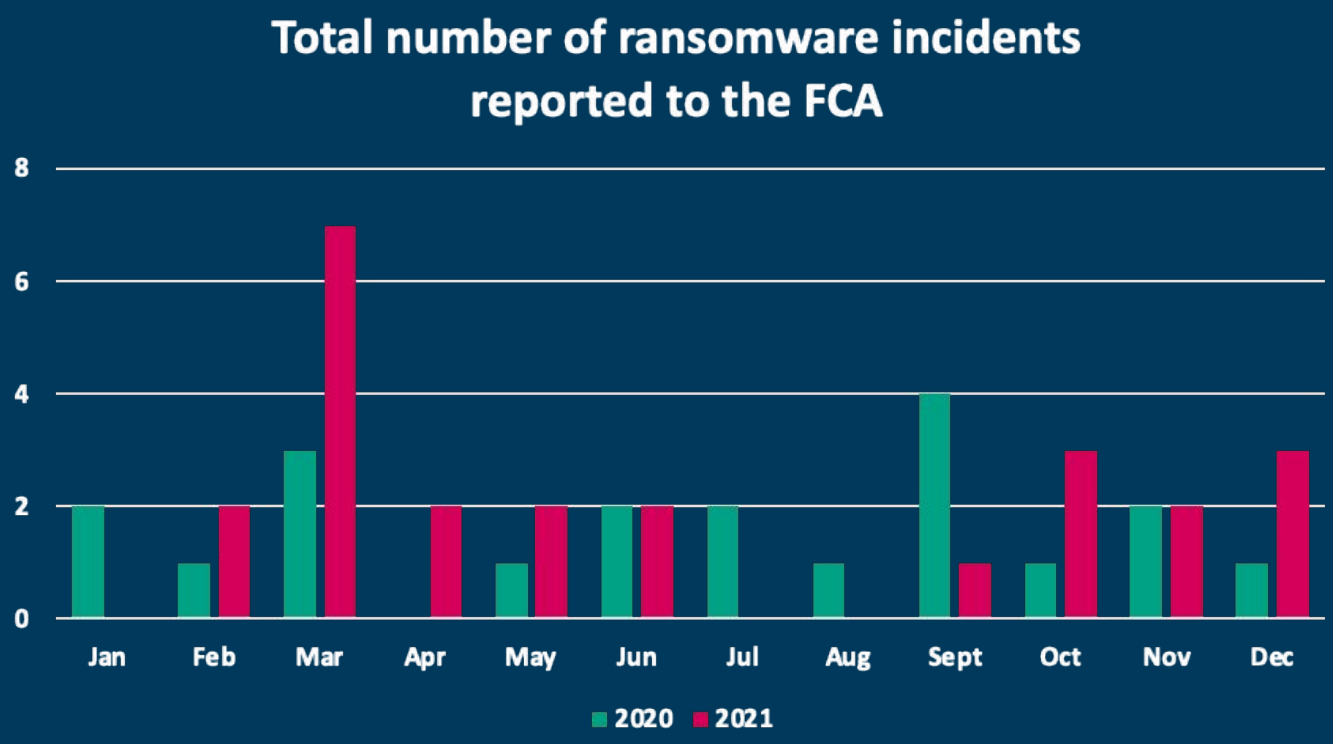
4. The Growing Threat of Ransomware

In 2021, high profile ransomware attacks on organisations such as the Colonial Pipeline Company and Ireland's Health Service Executive made news headlines around the world due to the large-scale damage and disruption they caused.

More than a quarter of the material cyber incidents reported to the FCA in 2021 involved ransomware. This marks a 20% increase compared to the total number reported in 2020 and highlights just how prevalent the ransomware threat is to UK firms.

Big game ransomware gangs such as Lazarus, Cobalt and Fin7 are known to target financial institutions and were all particularly active in 2021.

The increase in ransomware-related incidents in 2021 will be of cause for concern given that the average cost of a ransomware attack to UK finance firms is now £1.4m^.



*Source: www.computerweekly.com

5. A Spike of Incidents in Spring

There was a significant spike in material cyber incidents reported to the FCA in March 2021. 21 reports were filed to the FCA in total, more than double the 2021 monthly average. The number is triple that reported in March 2020 (7), when security experts warned that cybercriminals would act swiftly to take advantage of the global pandemic and remote working.

March 2021 cyber incidents

March 2020 cyber incidents

As to why data breaches in March 2021 were so high, we've contacted the FCA for comment but are yet to receive a response. Picus Labs researchers suggest that the spike may be explained by threat groups, including the China-based Hafnium gang, exploiting the highly publicised Microsoft Exchange Server vulnerabilities around this time.

In early March 2021, Microsoft released four out-of-band security updates due to the active and widespread exploitation of vulnerabilities in on-premises Exchange servers. The vulnerabilities allowed threat actors to read sensitive information in emails, take control of a compromised server, collect and exfiltrate data, and move laterally through a network.

On 7th March 2021, The European Banking Authority (EBA) announced that it had been the subject of a cyber-attack against its Microsoft Exchange Servers and Picus Labs researchers believe that attack campaigns are likely to have affected thousands of other organisations across the finance sector.

6. Final Thoughts

Our FOI data from the FCA highlights the extent to which the finance industry continues to be affected by cyber incidents. More than 110 material cyber incidents were reported by organisations to the regulator last year.

Given the financial and reputational damage that incidents can cause, it is important that all organisations, regardless of their cyber maturity, continuously assess the effectiveness of their security controls and processes. This is in order to better defend against external threats as well as those that originate from within.

Another research study by Picus Security, **The Red Report 2021,** reveals how regularly threat actors continue to vary their approaches. Only by proactively testing prevention and detection capabilities against the latest attack techniques will organisations across the finance sector be able to better understand where their security gaps are and take swifter action to mitigate them.

Suleyman Ozarslan, Co-founder of Picus Security and VP of Picus Labs:

"Financial services firms are amongst the best prepared and most highly capable organisations at detecting and responding to cyber incidents. Yet, despite investing heavily in security and data protection, it's clear that many continue to experience challenges in these areas.

"The large rise in cyber incidents reported to the FCA in 2021 is a concerning trend and should serve as an important reminder to all firms about the need to make ongoing improvements in all areas of security. This is necessary to not only mitigate the risks posed by external threats but also those that arise due to IT failures and human error.

"Just like most organisations, firms in the financial sector have been embracing new technologies and adapting to remote working. On top of this, they have had to contend with being a target of Advanced Persistent Threats and ransomware operators, as well as manage the risks of critical vulnerabilities in widely used systems such as Microsoft Exchange Server.

"Only by challenging their defensive capabilities on a continuous basis can firms hope to measure their threat readiness more accurately and swiftly close the gaps needed to take their operational resilience to the next level."

7. Appendix

FOI RESPONSE FROM FCA

Freedom of Information: Right to know request

Thank you for your request of 14 January 2022, in which you asked:

A. *Please can you provide information on the total number of material cyber incidents reported to the FCA between the period 1st January 2021 and 31st December? Please provide this data broken down by month. The FCA previously defined a material cyber incident here.*

B. *Of the total number of material cyber incidents reported (answer to question A), how many of these were cyber-attacks? Please provide this data broken down by month.*

C. *Of the total number of material cyber incidents reported (answer to question A), how many contained notifications where the confidentiality of company or personal data may have been compromised or breached? Please provide this data broken down by month.*

D. *Of the total number of material cyber incidents reported (answer to question A), how many involved ransomware? Please provide this data broken down by month.*

E. *Of the total number of material cyber incidents reported in 2020, how many involved ransomware? Please provide this data broken down by month.*

We have processed your request in line with the provisions of the Freedom of Information Act 2000 (FOIA) and our response is below.

Appendix

Question A

Month 2021	Number of cyber security incidents reported as cyber attacks
January	9
February	10
March	21
April	13
May	10
June	10
July	7
August	5
September	10
October	9
November	7
December	5
Total	**116**

Please note that we hold centralised records of major operational incidents reported to the FCA by individual firms under SUP 15.3 and Principle 11. These records include incidents that are a result of cyber-attacks.

These records, however, do not include cyber incidents at FCA regulated firms which have not been reported directly to the FCA.

Please note that the above data is accurate as at 26 January 2022 but are subject to change due to ongoing investigations of incidents.

Appendix

Question B

Month 2021	Number of cyber security incidents reported as cyber attacks
January	4
February	6
March	12
April	10
May	8
June	7
July	4
August	3
September	4
October	7
November	6
December	4
Total	**75**

Of the cyber incidents reported to the FCA in 2021, as outlined above in point A, the following were identified as being a result of a cyber attack.

Appendix

Question C

Month 2021	Number of cyber security incidents that involved a data breach
January	2
February	1
March	2
April	7
May	6
June	7
July	2
August	4
September	2
October	1
November	1
December	2
Total	**37**

Of the 116 cyber incidents reported to the FCA in 2021, 37 cyber incidents involved a data breach. Due to the nature of cyber incidents, this number is subject to change should further information be identified that indicates the occurrence of a data breach.

Where a firm has notified the FCA of a cyber-attack, the FCA will assess whether the incident involves a breach or compromise of company and/or personal data from the initial incident report provided by the firm – at which point the firm will be reminded of their obligation to report to the ICO.

Appendix

Question D

Month 2021	Number of cyber security incidents that involved ransomware
January	0
February	2
March	7
April	2
May	2
June	2
July	0
August	0
September	1
October	3
November	2
December	3
Total	**24**

By way of context, where a firm notifies the FCA of a cyber-attack, the FCA records the root cause component of those cyber-attacks in one of the following ways:

- Cyber – 3rd Party
- Cyber – Malware
- Cyber – Phishing
- Cyber – Ransomware

The above table contains the number of incidents which were reported to the FCA and recorded using the 'Cyber – Ransomware' tag.

Appendix

Question E

Month 2020	Number of cyber security incidents that involved ransomware
January	2
February	1
March	3
April	0
May	1
June	2
July	2
August	1
September	4
October	1
November	2
December	1
Total	**20**

About PICUS

At Picus Security, we help organisations to continuously validate, measure and enhance the effectiveness of their security controls so that they can more accurately assess risks and strengthen cyber resilience.

As **the pioneer of Breach and Attack Simulation (BAS),** our Complete Security Control Validation Platform is used by security teams worldwide to proactively identify security gaps and obtain actionable insights to address them.

www.picussecurity.com

picussecurity