HISCOX

CYBERCLEAR®

Global claims update
January to March 2021

Critical vulnerabilities drive claims numbers up

In a pattern similar to Q1 last year, a large number of critical vulnerabilities made headlines and caused a significant number of claims notifications early this year. In February, the Accellion Zero Day was exploited by a ransomware gang that stole data through its file transfer application (FTA) server.

However, in early March, the Microsoft Exchange Zero Day exploit made much bigger waves followed by the F5 networks vulnerabilities. All three, especially Exchange, are widely used tools requiring a number of companies to review and address these vulnerabilities.

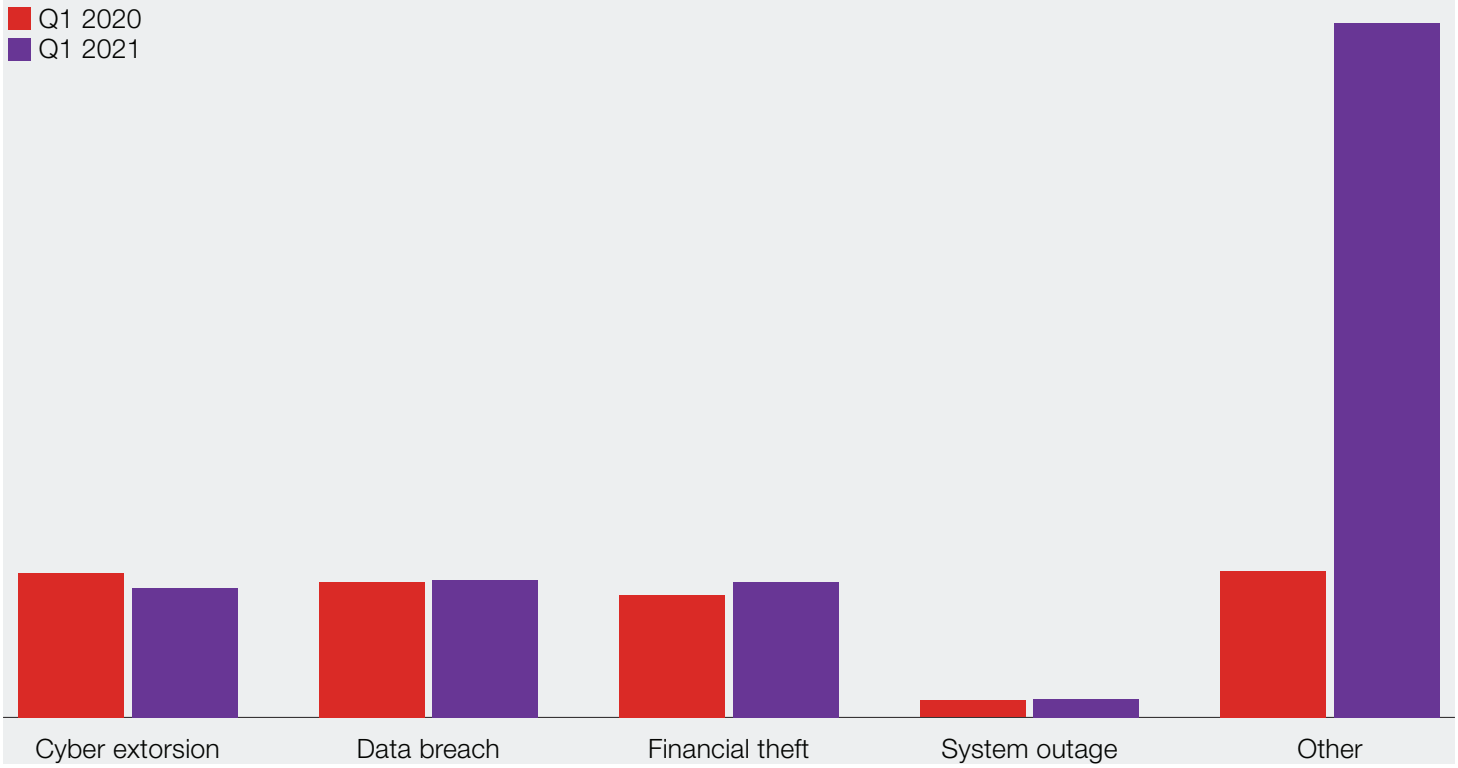
In the Hiscox top risks for 2021, we noted that remote desktop protocol (RDP) ports, lack of patching, and virtual private network (VPN) vulnerabilities were major causes of ransomware in 2020. Additionally, Microsoft released notifications for a number of vulnerabilities that required massive patching efforts to resolve. We projected the challenge of recognising and managing vulnerabilities would continue into 2021, and unfortunately we've seen even more vulnerabilities in the first few months of the year.

The most frequent claims for Hiscox in Q1 2021 involved 'other' (which includes incidents such as exploited vulnerabilities, telephone hacks, data destruction, cryptojacking), data exfiltration and financial theft. Overall, the total number of claims almost doubled from the previous quarter. UK, Europe and USA increased by 13%, 179% and 29% respectively. This jump in the number of 'other' claims was due to a large number of Microsoft Exchange vulnerability notifications (40% of overall claims), which mostly came from Europe. Though these claims were high in frequency, they were low impact.

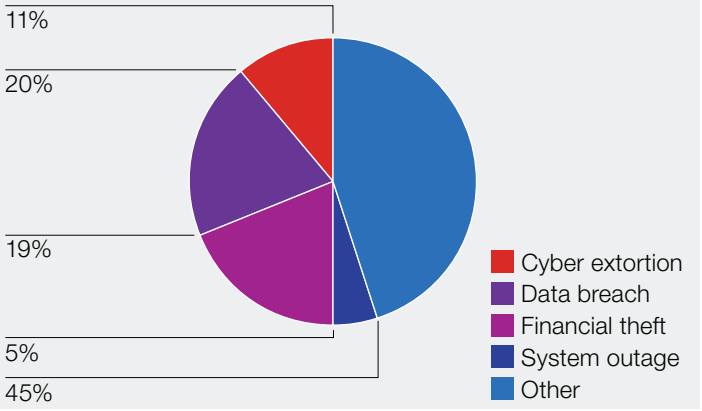
About a quarter of all ransomware claims were confirmed to include at least some data exfiltration by threat actors. Sodinokibi was the most common variant followed by Conti, Ryuk and Lockbit. There were multiple incidents of supply-chain attacks, especially ransomware attacks, on insureds' managed service providers (MSPs). Thirty-one percent of such attacks led to business interruption while 56% resulted in data breach claims.

From an industry standpoint, 22% of all data breach claims in the USA involved the healthcare sector and a breach of HIPAA or protected health information (PHI). Excluding the Microsoft Exchange incident, 12% of all claims involved phishing and another 12% involved business email compromise (BEC).

Claims impact comparison (%)

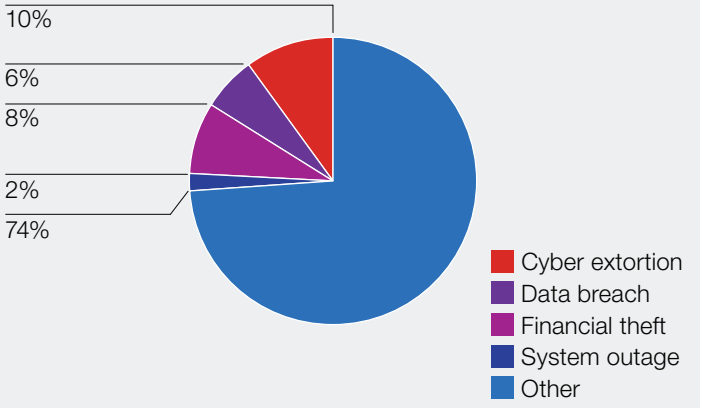


Claims impact by geography – UK



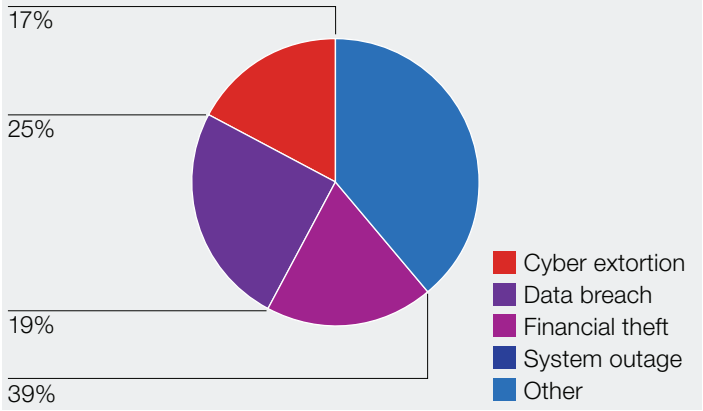
- Thirty-three percent of claims in February were as a result of BEC and/or phishing.
- Twenty-eight of total claims in March were Microsoft Exchange vulnerability notifications.
- Two-thirds of data breach claims were as a result of accidental disclosures by employees.

Claims impact by geography – Europe



- About a quarter of the claims in January were as a result of ransomware attacks. Almost half (45%) of these ransomware attacks were confirmed to have open RDP ports as the entry point.
- Twenty percent of January claims were as a result of BEC and/or phishing
- Over three-quarters (76%) of total claims in March were Microsoft Exchange vulnerability notifications.

Claims impact by geography – USA



- Seventeen percent of claims in January were as a result of ransomware attacks.
- Most ransomware attacks in February included data exfiltration.
- In March, 28% of total claims were Microsoft Exchange vulnerability notifications.

Real-life attacks

IT services
Revenue: €100 million
Impact: data breach

An IT consultancy suffered a data breach and they didn't even know it. The insured was contacted by a security consultant who notified them that the personal data of customers was publicly visible on their recently created website. The personal data affected included: names, bank account name and email addresses.

Real estate management
Revenue: €2.5 million
Impact: cyber extortion

A real estate management company suffered a Lockbit ransomware attack after threat actors exploited the Microsoft Exchange vulnerability on one of their servers. All data was encrypted by the hackers and systems were completely down for days.

Internet service provider
Revenue: €43 million
Impact: cyber extortion and system outage

A company that supplies fibre, wireless, voice, and managed services was hit with a DDoS attack and ransomware demand. A warning was given seven days prior, allowing the response team to assist the business in defences and protecting data. The attack occurred with minimal down-time.

Mitigate your risks

- Microsoft Office 365 compromise is still a problem, causing business email compromise (BEC) and payment diversion fraud (PDF) cases in the USA and Europe. It's essential to ensure multi-factor authentication is activated, especially on all administrator accounts.
- Remote desktop protocol (RDP) is heavily relied on by many organisations for remote working, but it still remains the most common point of entry in ransomware attacks. Ensure these tools are set up properly, kept up-to-date and patched against vulnerabilities as quickly as possible.
- Hiscox continues to see an increase in early notifications from insureds who have detected malware, a disclosed vulnerability or suspicious activity on their network. This is good practice for minimising risk. Such incidents (e.g. Microsoft Exchange vulnerability) when managed quickly helps prevent further attacks like ransomware as certain malware act as a precursor to such an attack.

Glossary

Cyber terms are often alphabet soup. We're here to help remind you what it all means.

Cyber extortion
Cyber criminals encrypting a victim's data/systems (ransomware), threatening to publish stolen data, holding data/systems hostage etc. until the victim meets their demands for payment.

Data exfiltration
Unauthorised access to data and in most cases, removal or copying of that data from the victim's network.

Distributed denial of services (DDoS) attack
An attack where multiple compromised systems are used to flood a target with network traffic, thus causing the targeted network to experience an outage.

Financial theft
Cyber crime involving the theft of money.

Payment diversion fraud (PDF)
Cyber criminals redirecting payment(s) to a fraudulent account.

Business email compromise (BEC)
Unauthorised access and control of a business email account which may lead to a data breach or payment diversion fraud.

Hiscox
1 Great St Helen's
London EC3A 6HX

T +44 (0)20 7448 6000
E enquiries@hiscox.com
hiscoxgroup.com

Hiscox, the international specialist insurer, is headquartered in Bermuda and listed on the London Stock Exchange (LSE:HSX). There are three main underwriting divisions in the Group – Hiscox Retail (which includes Hiscox UK & Europe, Hiscox Guernsey, Hiscox USA and subsidiary brand, DirectAsia), Hiscox London Market and Hiscox Re & ILS. Through its retail businesses in the UK, Europe and the USA, Hiscox offers a range of specialist insurance for professionals and business customers, as well as homeowners. Hiscox underwrites internationally traded, bigger ticket business and reinsurance through Hiscox London Market and Hiscox Re & ILS. For more information please visit www.hiscoxgroup.com.

20538c 06/21