HISCOX

CYBERCLEAR®

Global claims update
April to June 2020

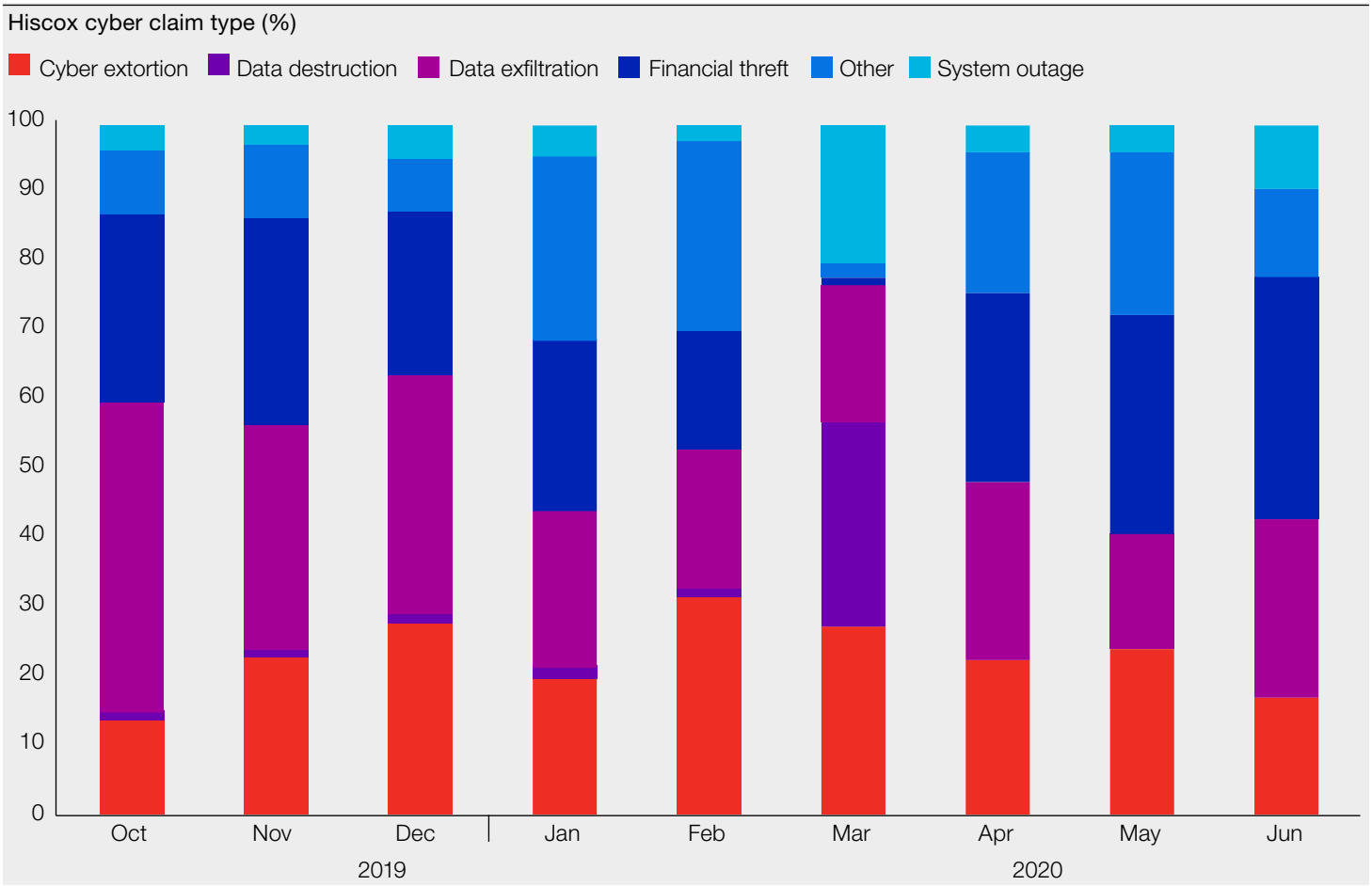
Claims frequency decreasing, while ransomware increasing

Data through June 2020 illustrates the immediate and continued impacts of COVID-19 on cyber claims. Overall, Hiscox cyber claims for businesses under £7.9 million in revenues decreased across the USA, UK and Europe by 17% from Q1 to Q2. The most significant change was in the UK with a 25% decrease, followed by an 15% decrease in the USA and 12% in Europe. On the other hand, large public organisations (£3.9 billion+ revenue, listed on a US stock market) have seen more ransomware incidents in H1 2020 than the whole of 2019 and we expect this to at least double by the end of the year.

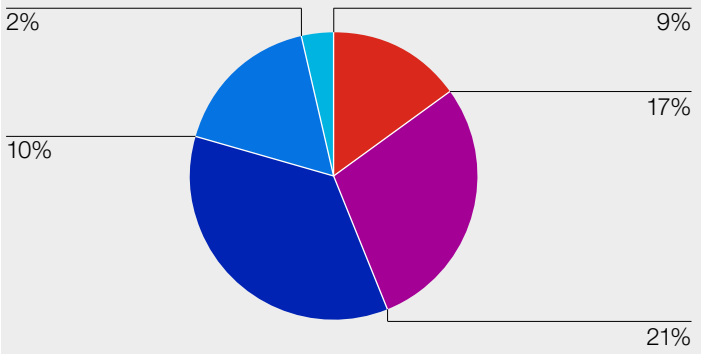
Certain risks had a significant impact on Q2 claims, specifically financial fraud. Financial fraud was the highest claim impact across all geographies in Q2 with a staggering 67% increase from Q1. Europe experienced three times as many financial theft claims than in Q1, while the USA saw a 29% increase. Payment diversion fraud was the primary tactic used in successful financial fraud attempts, and remote working due to COVID-19 may have played a key role. Normal processes and procedures for vendor payments and approvals may not have been followed given the current climate. Additionally, compromised third parties could have caused a breach. Either way, it's important to understand one's current coverage and add additional crime cover, if necessary, to mitigate risks like payment diversion fraud or other forms of financial theft.

New ransomware gangs have also cropped up. In Q2 2020, the most prevalent ransomware strain for Hiscox claims in the USA and Europe was Dharma. Other common strains included Snatch, Maze, LockBit and Medusa. The pandemic seems to have affected ransomware claims in both positive and negative ways. For example, a hotel suffered a ransomware attack which had very minimal impact since operations were already shut down, leading to no BI loss. For another insured, however, they were out of luck after a ransomware incident because their backups were dated two months prior. Movement restrictions led to a lockout in the location where the back-ups were located during the lockdown months. But it's not just about an individual company experiencing ransomware. Like financial fraud, third-party vendors and supply chain structures are important to secure. In April, 44% of US ransomware claims were the insured's vendor suffering the attack, thereby affecting the insured.

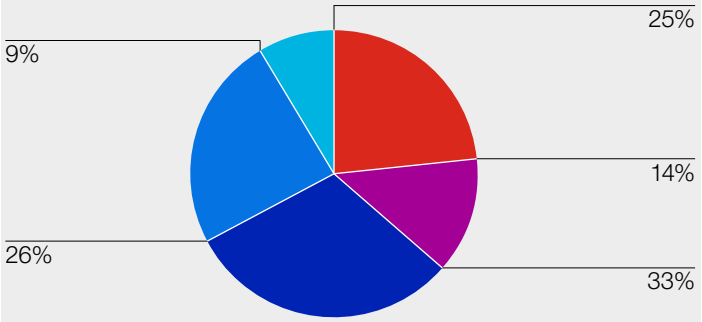
Nine-month and geographic views



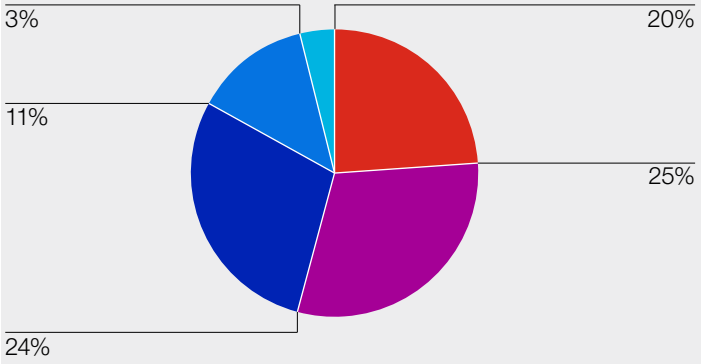
UK Q2 2020 claims (%)



Europe Q2 2020 claims (%)



USA Q2 2020 claims (%)



Mitigate your risks

- Microsoft Office 365 (O365) compromises are still problem, causing many of the business email compromise (BEC) and payment diversion fraud (PDF) cases during Q2 in the USA and Europe. Ensure multi-factor authentication is in place, especially for O365 administrator accounts.
- RDP and VPN remain the common points of entry in ransomware attacks. These are technologies that are heavily relied on, especially for remote working. Such incidents can be prevented by consistent patching.
- Last quarter, Europe insureds were really good at early notifications of potential claims. The USA and UK are now starting to do the same. It's important for businesses to notify their insurance carrier when they have detected malware or suspicious activity on their network. Because certain malware often act as a precursor to ransomware, a support team can assist right away to help prevent further attacks. According to the Hiscox Cyber Readiness Report 2020, whether a ransom was paid or not, the mean losses for all firms subjected to a ransomware attack were nearly twice as much as those that only had to grapple with malware on its own – £722,000 compared with £383,000. As cases of data exfiltration continue to increase, backups are no longer a fool-proof way to mitigate against ransomware attacks, you want to keep malware from becoming ransomware.

Real-life attacks

E-commerce
Revenue: £1.6 million
Impact: data exfiltration

An e-commerce platform providing home décor items was attacked, and the criminal obtained valid credentials to their Magento system, the ecommerce platform that powers their website. The hacker placed a script in the menu, which triggered when customers clicked on an invisible button placed on top of the checkout button. Once the script was triggered, it started collecting the check-out data from the customer, including name, address, shipping, billing, and credit card info.

E-commerce
Revenue: £122 million
Impact: data exfiltration

An online marketplace for art and graphic design services became aware through a media report that a hacking group had acquired data from several different companies, including them. The data was being sold on the dark web. The hackers obtained the data for millions of platform users, including customer names, login credentials and passwords. For some users, the information exfiltrated included birth dates, telephone numbers, billing, and shipping addresses.

Media
Revenue: £13.2 million
Impact: cyber extortion

A media agency suffered a ransomware attack of the RagnarLocker variant. During a forensic review, it was discovered that the criminals also stole the personal information of the insured's customers. The ransom demand of £934,000 was negotiated to £177,000 and paid.

Wholesale supplier
Revenue: £4.6 million – £9.2 million
Impact: financial fraud

A vehicle parts supplier suffered a payment diversion fraud (PDF) attack after an employee's email was compromised and used to send customers emails containing wrong payment details. In total, customers ended up sending £47,000 to the hacker.

Food wholesale
Revenue: £17.9 million
Impact: cyber extortion

A food wholesale supplier suffered a ransomware attack of the Dopplepaymer variant. The ransom demand was £70,000 which was paid, In addition, the insured suffered over £78,000 in business interruption losses.

Finance
Revenue: £2.8 million
Impact: cyber extortion

A debt collection agency suffered a ransomware attack with data exfiltration. Attackers requested 44.9 BTC (£350,000) in order to restore systems and not leak the data they had exfiltrated. There was some very sensitive information (medical records and personal financial info) contained on the insured's databases with about 350,000 data subjects exposed.

Educational services
Revenue: £1.6 million
Impact: financial theft

An educational institution suffered a business email compromise (BEC) with payment diversion fraud (PDF) amounting to £15,400. The attackers were also likely to have had access to sensitive PII relating to minors. Initial investigations showed that six malicious emails were sent by the perpetrator attempting to convince recipients to send school fees to a fraudulent bank account, offering an 'early payment discount'.

Glossary

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

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

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 a victim's network.

Financial theft
Cyber crime involving the theft of money.

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

Remote desktop protocol (RDP)
A proprietary tool developed by Microsoft which provides a user with an interface to connect to another computer over a network connection.

VPN (virtual private network)
Commonly used to allow remote workers that are outside the corporate network to securely access corporate services from home or while travelling.

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.

20538a 09/20