HISCOX

CYBERCLEAR®

Global claims update
July to September 2020

Increase in claims driven by data exfiltration

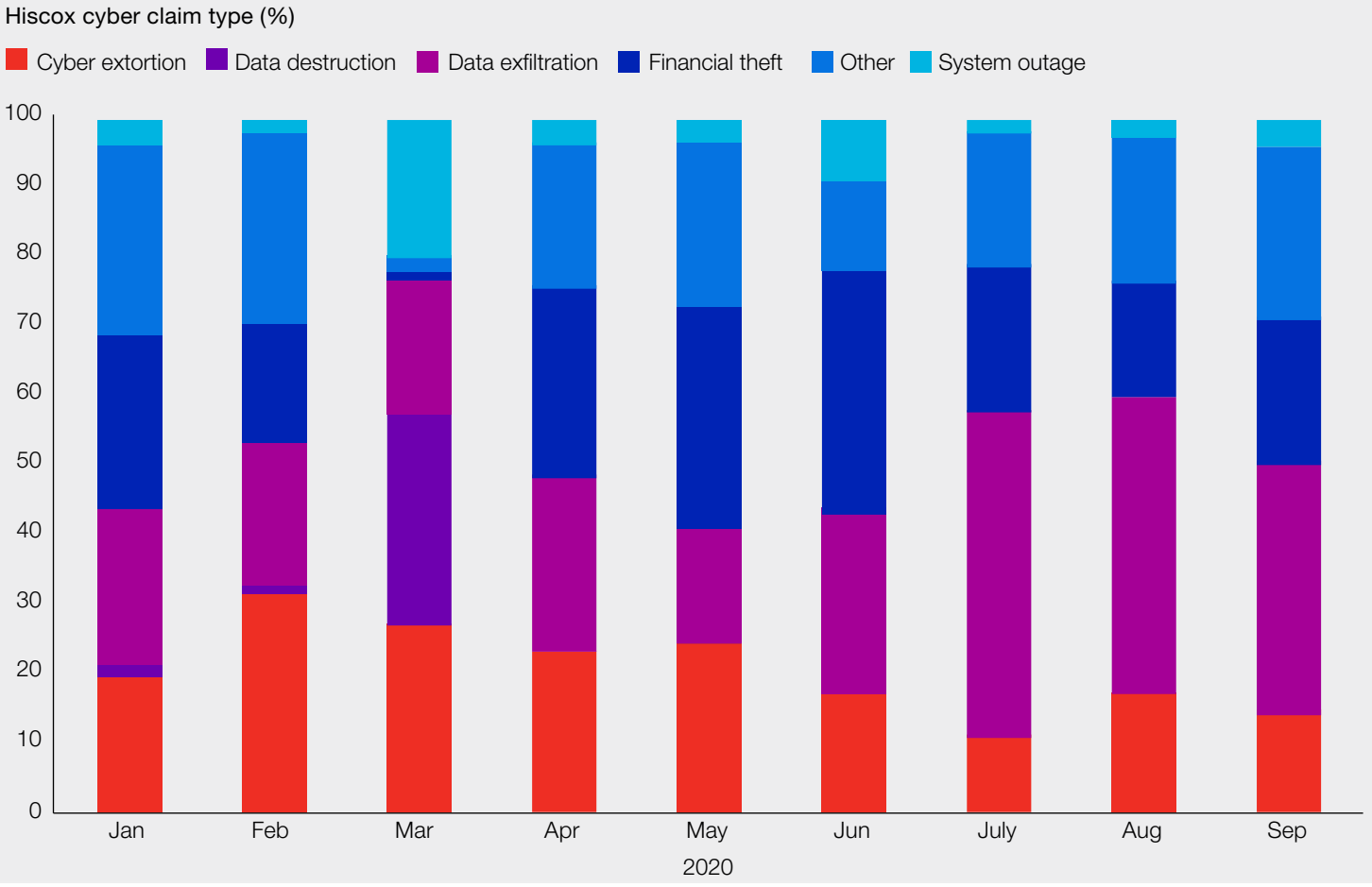
The third quarter of 2020 had the most claims over the last four quarters, a 49% increase compared to the previous quarter. UK, Europe and the USA increased by 73%, 29% and 57% respectively. Seventeen percent of claims were suffered in month(s) prior to the reported date. This delayed reporting was likely a result of the pandemic given the reduced number of claims in the first and second quarters.

Data exfiltration was the top incident type, specifically where customers suffered ransomware attacks with doxing. There was a staggering 189% increase in data exfiltration from Q2. An increase in incidents where vendors suffered ransomware attacks that affected their customers data drove these claims. The most prevalent ransomware strains were Maze and BitLocker. Other common strains include Sodinokibi, LockBit and Dharma. Victims received ransom demands of at least £1 million.

Since October 2019*, remote desktop protocol (RDP) and remote access were the point of entry for 61% of ransomware cases across all regions. The second-highest point of entry was phishing at 24%, and virtual private network (VPN) and managed service providers (MSPs)/third parties tied for third at 6% each.

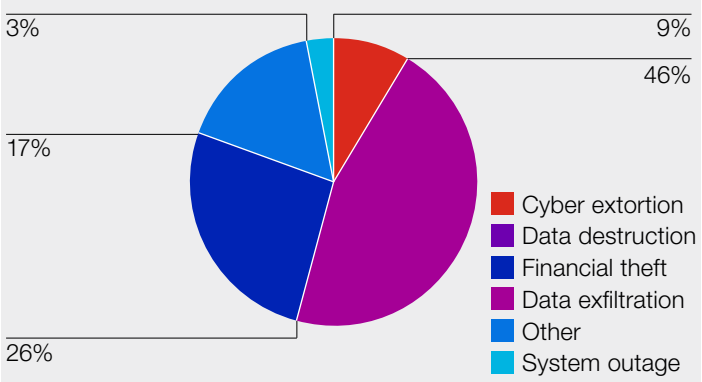
Looking at July 2020 alone, 50% of UK claims were data breaches. In Europe, a majority of the ransomware attacks were via open remote desktop protocol (RDP) ports. Business email compromise (BEC) and phishing emails were the major causes of data breaches. In the USA, two-thirds of claims were data exfiltration and 61% of these claims were as a result of the insured's vendors suffering ransomware attacks with doxing. Data exfiltration and doxing continued to be a theme throughout the quarter, most noticeably in the UK and USA.

Month over month and geographic views

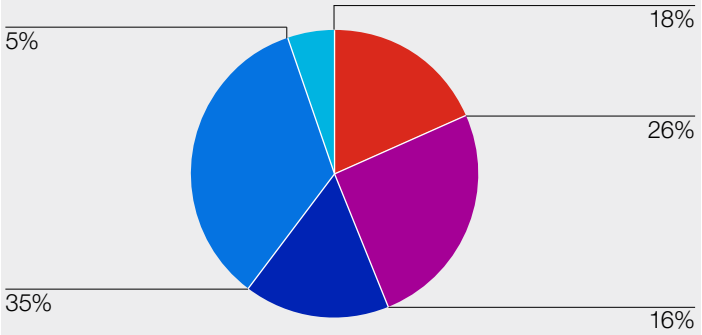


*This is a sample of 39% of ransomware cases across the period of October 2019 through September 2020 where point of entry could be confirmed.

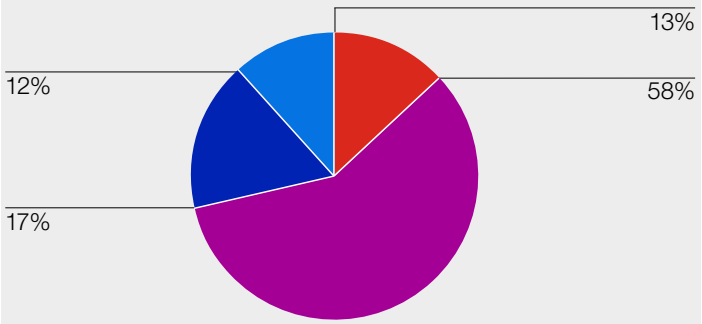
UK Q3 2020 claims (%)



Europe Q3 2020 (%)



USA Q3 2020 claims (%)



Mitigate your risks

- Microsoft Office 365 compromises continue to be the root cause of many BEC and payment diversion fraud (PDF) cases in the USA and Europe. Ensure multi-factor authentication is in place, especially for administrator accounts.
- RDP remains the main point of entry in ransomware attacks and ultimately data exfiltration. When these ports are exposed to the internet, they offer a relatively easy way for criminals to enter a network. Such incidents can be prevented by patching, disabling ports (unless necessary), and limiting port exposure to the internet.
- Due diligence on supply chain vendors is essential, especially if they process insured's data. Doxing during ransomware attacks is now commonplace and will only continue to increase the number of data breach claims.

Real-life attacks

Manufacturing
Revenue: £31 million
Impact: cyber extortion

A rubber and plastic production company suffered a ransomware attack where the cyber criminals asked for a ransom of 28BTC (£251,000). Because the insured had such great backups, they were able to restore all data and avoid paying a ransom.

Charity
Impact: data exfiltration

A children's charity was notified by their cloud software provider that they had suffered a ransomware attack and the insured's data was stolen. The vendor confirmed they paid the cyber criminal's ransom demand in return for confirmation that the stolen data had been destroyed, but regulations still require notification.

Marketing
Revenue: £1.5 million
Impact: financial theft

A data supplier to technology vendors suffered a payment diversion fraud (PDF) attack. The insured made three payments totalling £83,000 to what they believed was their lawyers' account. It turns out that the lawyers were hacked and had their bank details changed. Thankfully, the insured had crime coverage and £73,000 of the lost funds were covered.

Professional services
Revenue: £245,000
Impact: data exfiltration

An accounting firm experienced a phishing attack that led to the business email compromise (BEC) of seven email accounts. The breach affected email correspondence with over 2,000 clients and impacted their personal information. The insured notified all potentially-affected clients after extensive data mining. Total costs for legal work, data mining, and notification costs was £96,500.

Professional services
Revenue: £598 million
Impact: data exfiltration

A single email account at a dental network experienced business email compromise (BEC) due to a security failure and data breach. That account held personal information for 24,000 people. The insured had to notify all affected data subjects per regulatory requirements, which cost £112,000. Even though only a single inbox was compromised, data mining by the criminal caused additional costs for a relatively small incident.

Professional services
Revenue: £4.4 million
Impact: cyber extortion

A title agent experienced cyber extortion. They were lucky that the ransomware demand was for a nominal amount. The insured was able to pay the demand and reschedule all closings, which limited the business interruption loss. There was still a £36,000 bill in total costs and potential reputational harm and lost clients.

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 the victim's network.

Doxing
This refers to the act of publicly disclosing or publishing data belonging to someone else without their permission.

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 12/20