HISCOX

CYBERCLEAR®

Global claims update
January 2020 to March 2020

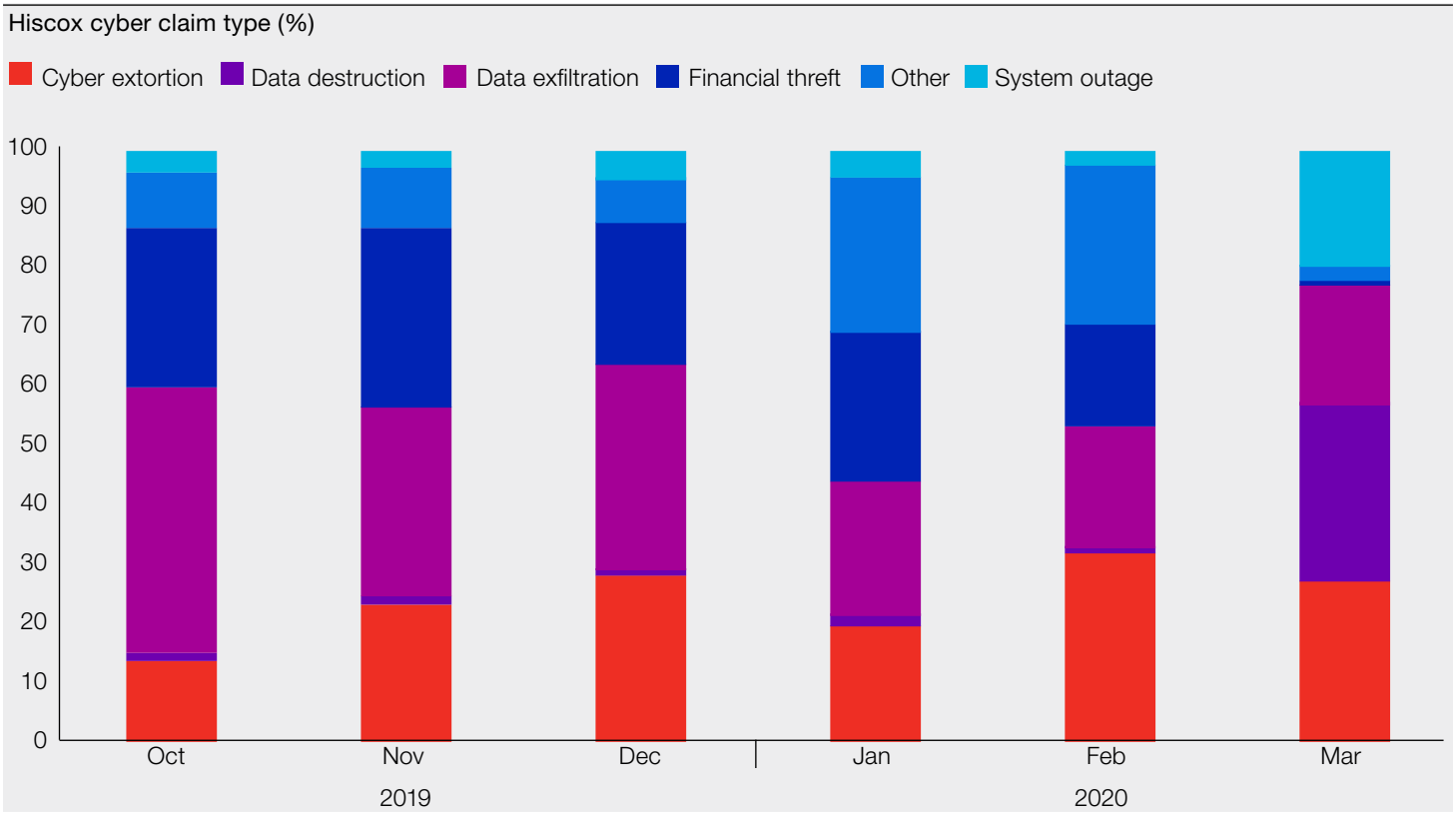
Claims decrease but new threats arise

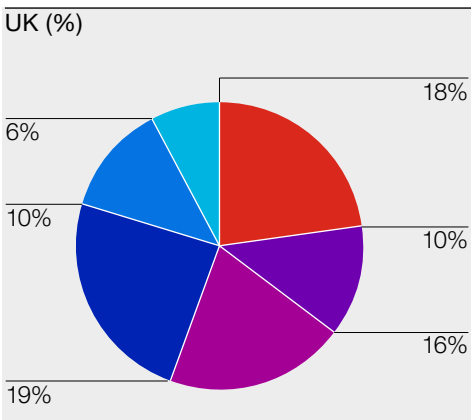
Over the last six months, there's been a slight decrease in Hiscox cyber claims across the USA, UK and Europe. The average claims per month over a three month period fell 7% between Q4 2019 and Q1 2020. The most significant change was in the USA with a 16% decrease, followed by 9% in the UK and an increase of 2% in Europe. The decrease in claims my be a result of widespread business lock-downs due to the COVID-19 pandemic. We'll see how this progresses as the year goes on.

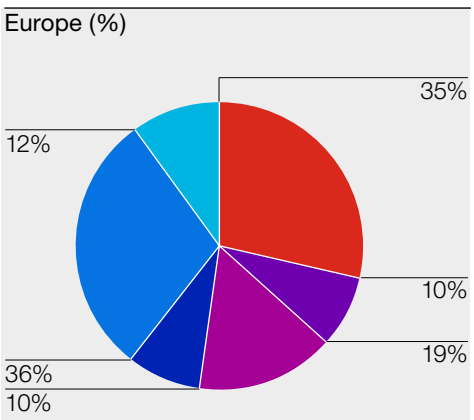
Data exfiltration continues to lead the charge as a key threat, however cyber extortion (ransomware) surpassed financial fraud in Q1 2020. There was a spike of claims in February due to VPN vulnerabilities in Europe, which followed the publication of numerous known VPN vulnerabilities in January. Though generally low-severity claims, VPN vulnerabilities can be the entry point for larger, more destructive incidents.

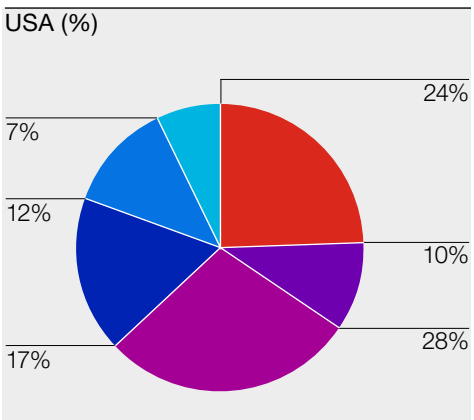
Better back-up practice allowed all our ransomware claims in Germany in Q1 2020 to be brought back online without paying a ransom. Ransomware gangs are adapting to this better back-up behavior and starting to exfiltrate and destroy data, rather than simply locking it. We saw a surge in data destruction and system outages in March, which follows this continued trend.

Six-month view









Real-life attacks

Marketing consultancy
Revenue: €44.6 million; **Claims cost:** €171,400
A marketing consultancy suffered a business email compromise. Funds meant for the company's client were diverted to the criminal's bank account. Thankfully, the diverted funds of $196,000 were recovered by the bank.

Management service provider (MSP)
Revenue: €75 million; **Claims cost:** €288,364
An MSP suffered a ransomware attack. The demand was €288,364 and the attackers threatened to increase every three days by a further €61,168. The most recent backups were from July 2019 and the MSP was forced to pay the ransom.

Charity
Revenue: €35 million; **Claims cost:** €87,383
A company suffered a ransomware attack after an employee used an old laptop to log on remotely. In response to the COVID-19 lockdown, an employee was given a laptop that had dormant ransomware still present. Once the laptop was connected to the network, the ransomware unknowingly spread.

Repairman
Revenue: €119,765; **Claims cost:** €5,399
A repairman suffered a denial-of-service attack that that blocked his or her website for several days. The repairman managed getting forensic work completed. It was determined the cause of the attack was due to unusually high incoming traffic on the website, causing the server to crash. Action was taken to improve the firewall system, which helped diminish the traffic.

Food producer
Revenue: €77.8 million; **Claims cost:** €548,328
The insured was victim of a RYUK ransomware attack. All servers and backup files were encrypted. The insured was unable to take orders, ship products or invoice customers. Hiscox instructed a panel IT forensic vendor to negotiate ransom payment. Forensic investigation concluded that no personal information was downloaded or exfiltrated.

Construction
Revenue: €588 million; **Claims cost:** €48,061
The client reported a hacking attack due to unknown IP addresses attempting to log into company's employee-facing VPN. Hiscox inquired as to how certain the company was that an unauthorised person gained access, to which head of IT advised that the company couldn't be certain. Hiscox recommended an IT forensics investigation. This resulted in the conclusion that there was unauthorised access but no access to personal information. Thus, there was no data breach.

IT services
Revenue: €84.8 million; **Claims cost:** €2.1 million
A software engineering company reported a data center outage. All customer systems (mostly hosted web pages) were down, as well as the office data center at a branch. Since all IT systems were down, the insured required wide technical support. After forensics, it turned out a former employee gained access to the IT systems and caused enormous damage to all hosted data.

Golf club
Revenue: €3.1 million; **Claims cost:** €19,224
A golf club suffered from a ransomware attack that froze its entire server. This included the point of sales registers for the golf operations and the club restaurant. The insured was unable to retrieve or access their backups. Hiscox instructed forensics to establish if any data had been harvested by the ransomware or by the hacker. Furthermore, Hiscox paid the ransom after determining the threat to be genuine and the decryption key provided by the hacker would in fact release the server. The club's operations were restored and counsel concluded there were no data notification obligations.

Key cyber risk trends

VPN vulnerabilities emerge.
During the latter part of 2019, a number of VPN alliances have been found to have serious vulnerabilities. VPN devices need to be internet facing, which makes it easy for attackers to scan the internet for these vulnerabilities. These vulnerabilities give attackers remote access to a network without login credentials.

Payment diversion fraud continues to increase.
Over $8 million lost in PDF or social engineering claims (up from $6 million last quarter) with the USA accounting for at least 85% of these claims and less than 2% from Europe.

Sodinokibi is biggest ransomware threat.
It appears to be the most prevalent strain of ransomware especially in the USA and Europe (although limited data is available).

Ransomware attacks increasingly becoming data breach cases.
More ransomware claims involve data exfiltration, thereby increasing the costs.

Mitigate your risks

- **Train employees** to spot and manage phishing emails, as well as understand other cyber risks. Hiscox currently offers the **Hiscox CyberClear Academy**, a free cyber awareness training platform, to all of its cyber insurance customers. It includes modules on phishing, business email compromise (BEC), payment diversion fraud (PDF), managing supply chain risks etc.
- **Enable multi-factor authentication (MFA)** on user accounts, especially administrator accounts. Office 365 compromise is still a problem. BEC/PDF cases are prevalent, especially in the UK. MFA is a simple first-step towards securing email accounts.
- **Build a robust backup strategy** that will protect against ransomware attacks. Test it regularly. Forty-five percept of Hiscox European ransomware claims occur in Germany, who paid zero ransoms in this quarter as a result of adequate back-ups.
- **Patch all VPN hardware and software** and confirm it's up-to-date. If you run any such services and they have not yet been patched, please take them down to avoid being detected by internet scans. Also, reset authentication credentials of any affected VPNs.
- **Close all unnecessary open ports** to prevent being exploited by attackers. This is especially important for ports not associated with a known legitimate service. Ports which must remain open should be regularly monitored.
- **Update, update, update.** Ensure anti-malware software, IDS/IPS (Intrusion Detection/Prevention Software) etc. are up-to-date.
- **Notify your insurance carrier early** if you spot any anomalies on your network , such as malware. Malware can be to first step to larger attacks with increased costs. The earlier you notify of a potential claim or claim, the faster it will be to get your business back up and running.

Glossary

Cyber terms are often a jumble of letters. 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.

Financial theft
Cyber crime involving the theft of money.

Payment diversion fraud (PDF)
Cyber criminals redirecting payment(s) to a fraudulent account. Also known as social engineering.

Virtual private network (VPN)
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.

20538b 07/20