HISCOX

CYBERCLEAR®

Global claims update
January to June 2021

A quieter quarter for cyber claims

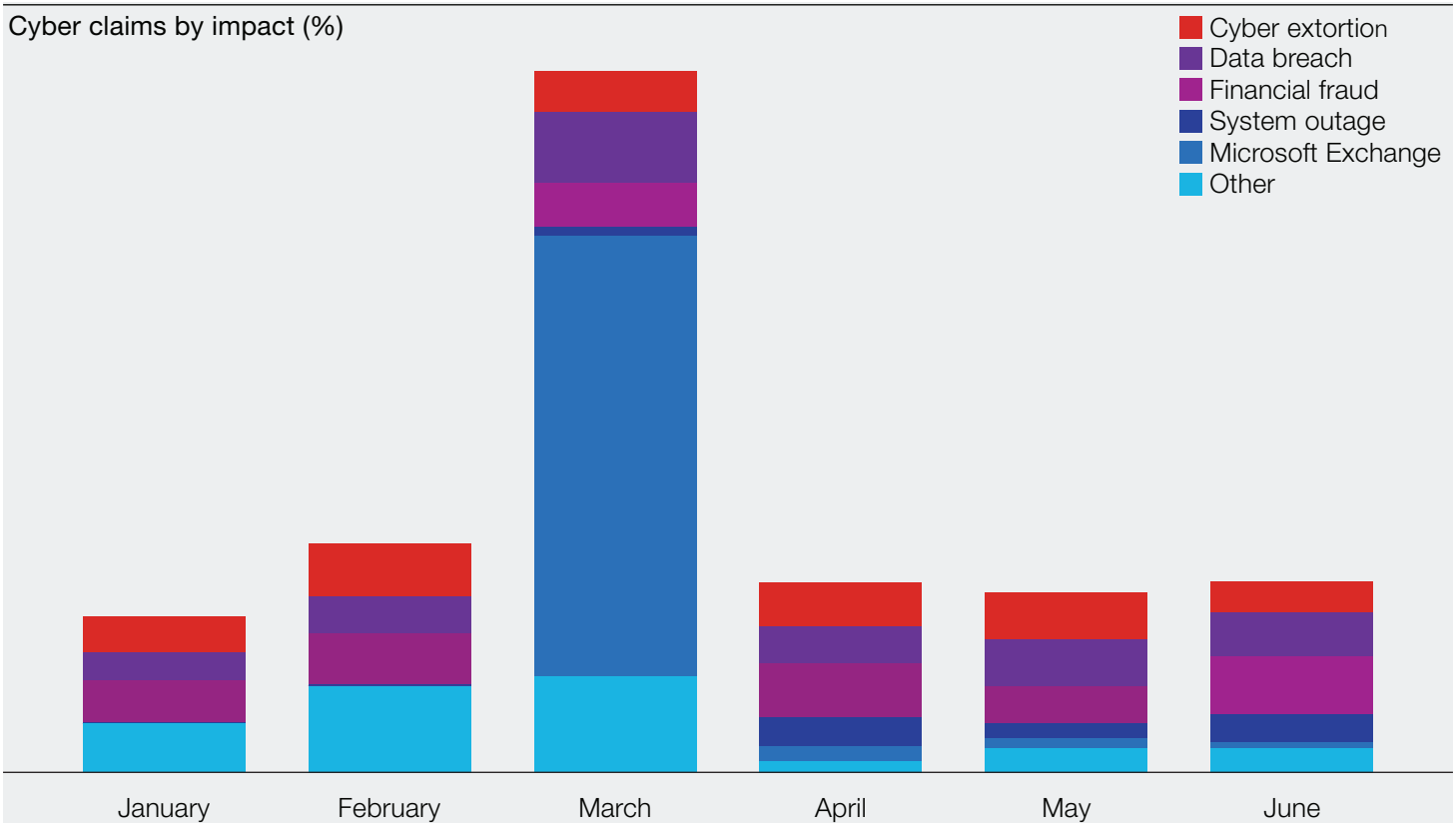
Large attacks like Microsoft Exchange made headlines in the first quarter of 2021. Comparatively, the second quarter of Hiscox cyber claims appears quieter for businesses with under $1 billion revenue across the USA, UK, and Europe. But the risks have not diminished.

In comparison to Q1, the number of cyber claims decreased by 93%, but claims increased by 52% when comparing the first six months of 2021 to the first six months of 2020. Microsoft Exchange (ME) vulnerabilities were a significant portion of Q1 claims, mainly affecting Europe and more specifically Germany. Even when the effects of ME are removed, however, claims still appear to decrease by 35% between Q1 and Q2 but increase overall by 37% when comparing last year to this year.

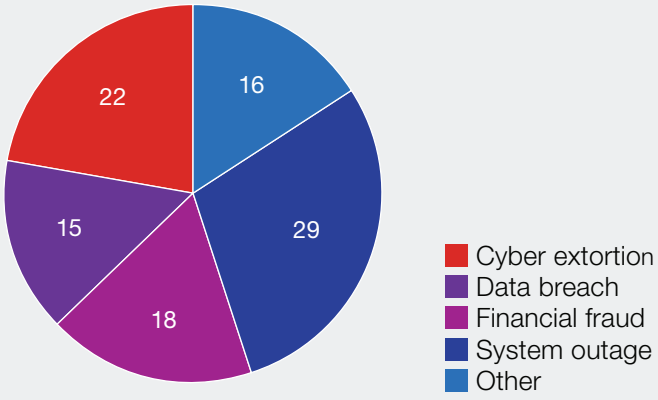
In the summer last year, new ransomware gangs and breaches were driving claims using Covid-19-related phishing campaigns. Though social engineering is still the main driver of claims (27% of attack entry points), thankfully cyber extortion did not drive claims impacts in Q2 2021. Twenty-seven percent were financial fraud, followed by 23% data breach, and 22% cyber extortion.

More government involvement in major ransomware breaches like Colonial Pipeline or Kaseya drove some ransomware gangs underground temporarily, but it appears they're merely regrouping and rebranding – Sodinokibi has become Lockbit and Avaddon evolved into Haron. There may be a lull in claims in Q2, but that doesn't mean it's a lasting trend.

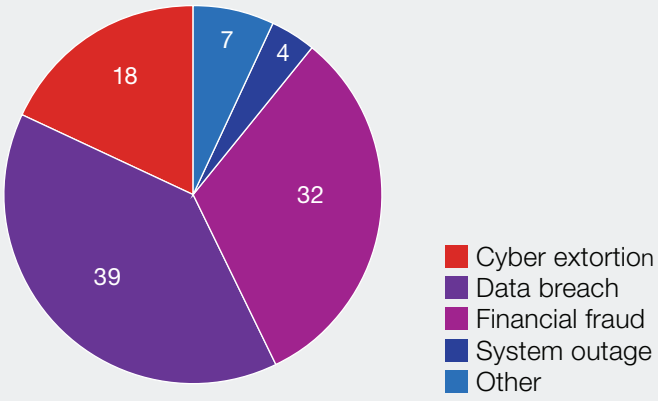
Our data this quarter highlights which points of entry seem to lead to certain impacts, as well as which impacts are costing the most. This type of insight builds awareness around where to focus cyber security priorities and spend, especially for smaller businesses, where security funds are often scarce.



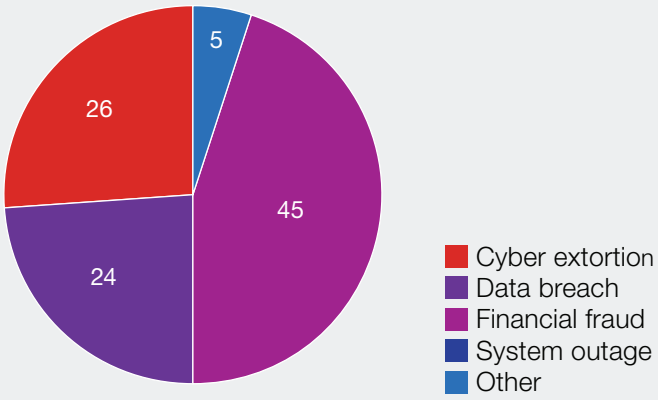
Europe (%)



UK (%)

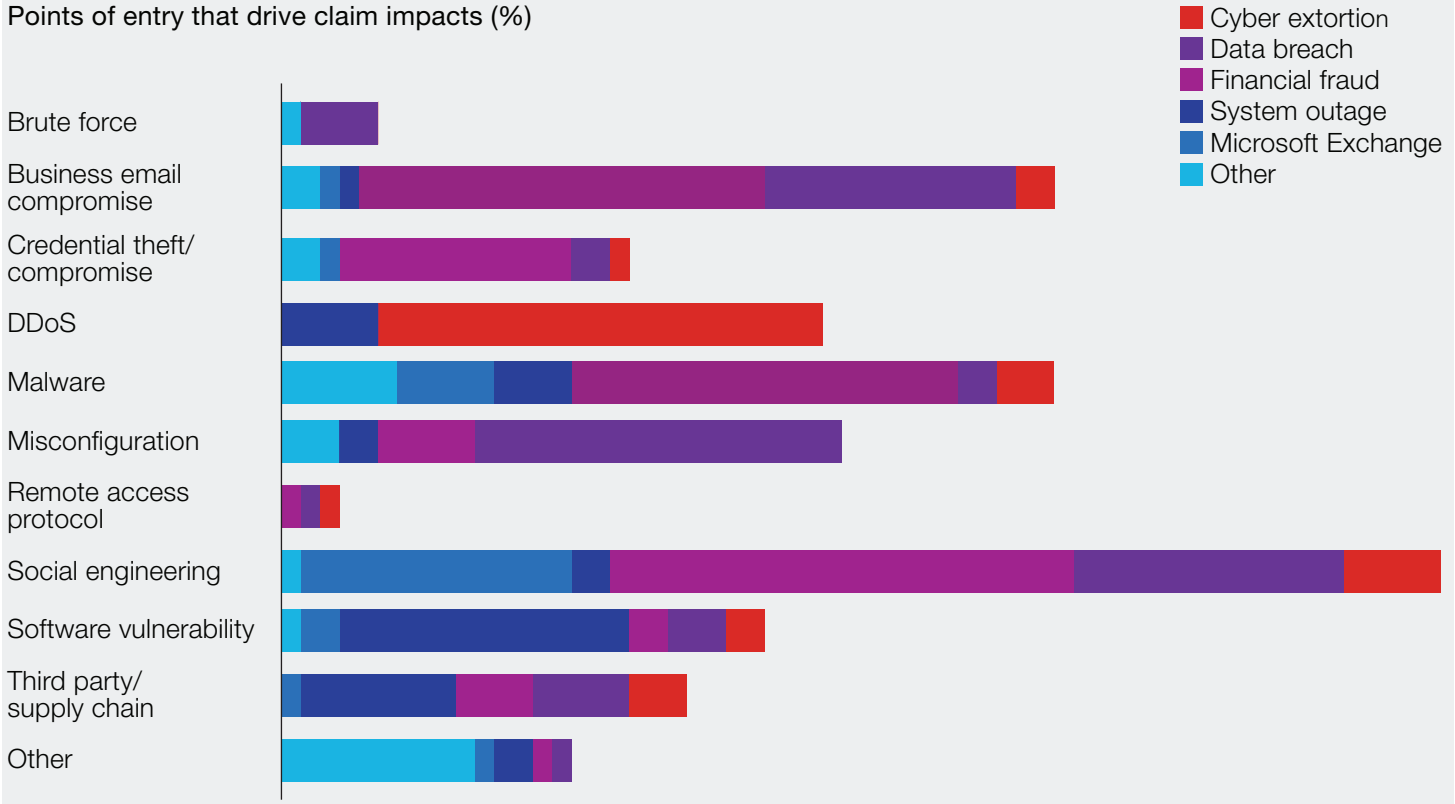


USA (%)



- By claims count, financial fraud and data breach were the most common type of incident. As in Q1, system outages remained the primary type of claims in Europe for Q2. The impact of the Microsoft Exchange vulnerability, however, was minimal.
- Data breach and financial fraud account for about two-thirds of the number of claims in the UK and USA. Where social engineering was found to be the point of entry, 87% of these attacks were caused by phishing and 7% by whaling.
- Cyber extortion drove most of the claims costs across all regions. For Europe, system outage also brought a high price tag. The UK and USA both incurred significant claims costs for financial fraud. The point of entry that created the most incurred claims costs was software vulnerabilities.

Points of entry that drive claim impacts (%)



- Social engineering was the main factor behind cyber extortion. There were a number of phishing claims that were reported, but did not become a major impact. Early reporting, even if a breach hasn't occurred, is essential in minimising damage.
- Thirty-percent of data breach claims were caused by misconfiguration and 22% by social engineering.
- Though social engineering was the main factor behind financial fraud (34%), business email compromise was also a major factor (30%).
- Software vulnerabilities were the primary cause of outages at 38%.

Real-life attacks

Accounting firm
Turnover: €855k
Impact: business email compromise

Twenty email accounts had passwords changed to gain unauthorised access from VPNs. Hackers accessed personally identifiable information (PII) of 27,000 individuals, requiring costs to notify the people affected. Data mining to review the 20 compromised email inboxes represented the bulk of the €188k costs.

Application service provider
Turnover: €30 million
Impact: data breach

Numerous laptops were stolen from the business premises. The laptops were unencrypted and contained client confidential information. Forensics established that almost 900 individuals needed to be notified and credit monitoring services initiated. Costs totalled €171k. This could have been mitigated if the portable device had at least 256-bit encryption and multi-factor authentication.

Financial services
Turnover: €11 million
Impact: cyber extortion

Because an insured's payroll vendor was the victim of a ransomware attack that impacted the insured's systems, they were unable to process payroll for ten days. This affected payroll, increased necessity for additional labour to be brought in, as well as caused a loss of clients. Thankfully, none of the insured's client data had been impacted. Legal counsel confirmed no confidential information was compromised by the ransomware so no notification obligations were triggered. Hiscox reimbursed the loss of income suffered by the company as a result of their vendor suffering a hack.

Mitigate your risks

- Business email compromise (BEC) was the second highest point of entry overall and payment diversion fraud (PDF) and other types of financial fraud was the second highest impact in the USA and UK. It's essential to ensure multi-factor authentication is activated, especially on all administrator accounts.
- Thirty-eight-percent of system outages were caused by software vulnerabilities. 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. When managed quickly, incidents like the Microsoft Exchange vulnerability incidents can be prevented from becoming further attacks like ransomware. Certain malware act as a precursor to such an attack.
- Build a human firewall by ensuring employees have adequate training. In cyber risks. Phishing attacks and financial fraud both commonly occur through phishing – 87% of social engineering was caused by phishing in Q2 2021 claims. Hiscox offers free cyber training to all Hiscox cyber customers through the Hiscox CyberClear Academy.
- Demand your vendors comply with good cyber security practice. Third-party vendors caused 16% of system outage claims.

Glossary

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.

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

21689c 10/21