HISCOX

CYBERCLEAR®

Hiscox Annual 2021 Claims Report

Introduction

Gareth Wharton
Cyber CEO
Hiscox

Awareness of cyber risk has grown significantly in the last couple of years. Between the increased risk of phishing campaigns around the pandemic in 2020 to the numerous vulnerabilities found in widely used software in 2021, mainstream media is clearly engaged in the cyber discussion.

The story in 2021 centers around supply chain vulnerabilities and how such large-scale impacts have pushed governments to more aggressively crack down on ransomware gangs. The March Microsoft Exchange vulnerability caused companies around the world to scramble, forcing businesses to prioritise updates and patching their core software. In May, Colonial Pipeline shut down operations because their payment software was hacked. The US government acted swiftly to trace funds to ransomware gang, Darkside, and disrupt further endeavors. An attack on national infrastructure finally led to a more public declaration for the importance of cyber security.

REvil's July attack on Kaseya, a Florida software company, illustrated how ransomware gangs have shifted strategies and impacted businesses across all sectors, size and region by exploiting vulnerabilities in their key suppliers. The supply chain, both the software a business uses and the more invisible suppliers their vendor might use, are under attack. So how did Hiscox fair?

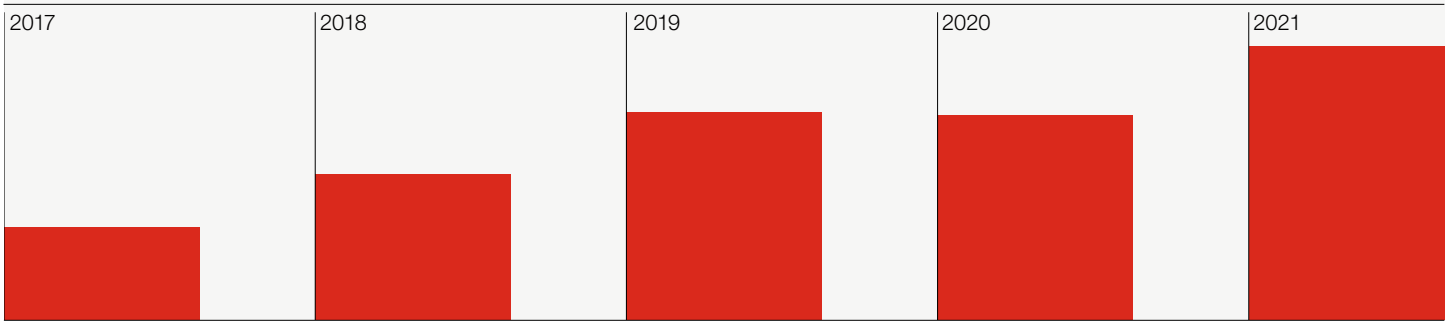
Total retail claims for small- to medium-sized businesses have increased 58% from the previous year. Claims in the UK, Europe and the USA rose 33%, 109%, and 14% respectively. The large surge in Europe was due in part to the Microsoft Exchange vulnerability. Cyber extortion and data breach were the most common types of claims in 2021.

Extortion losses have continued to grow, while losses for other claim impacts have significantly decreased. It's apparent that to reduce ransomware losses, taking preventative action is the most important factor. However, macro events, such as government pressure on ransomware gangs, did impact losses. Most extortion costs decreased in the second half of the year with the likes of REvil, Darkside, etc. going quiet.

Looking ahead, basic risk mitigation for companies and their supply chain continue to be important. Patching and updates are essential, and continued remote working makes the human firewall one of the greatest defenses against an attack.

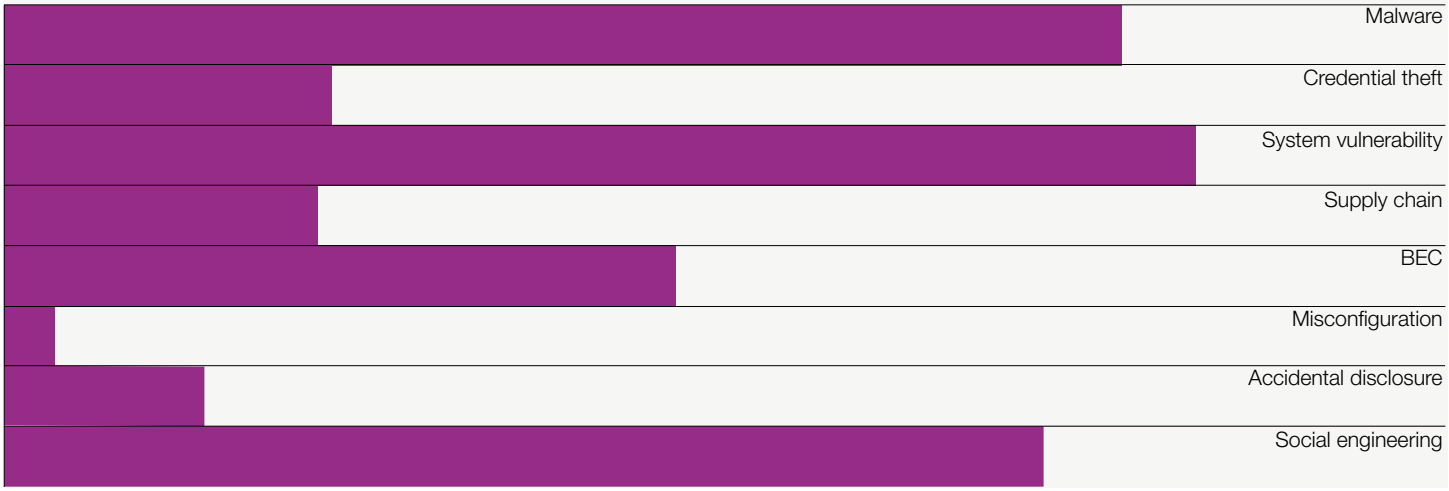
Cyber claims by numbers

Claims frequency growth
All Hiscox retail territories



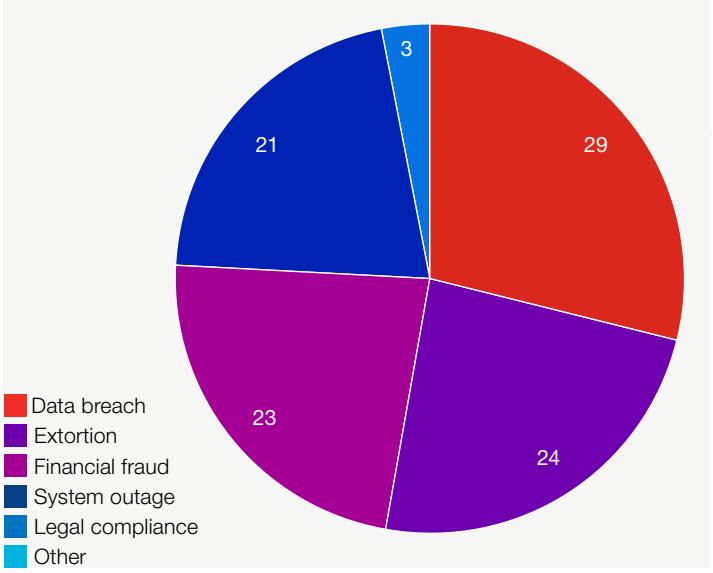
After a slight reduction in 2020, claim frequency increased again in 2021.

2021 claims causes
All Hiscox retail territories

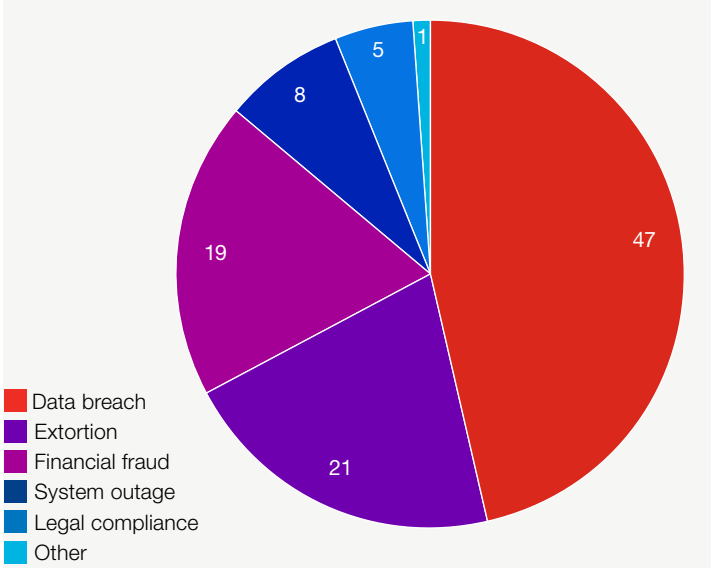


System vulnerabilities driven by the Microsoft Exchange incident in March 2021 were the most common cause.

2020 claims count by impact
All Hiscox retail territories

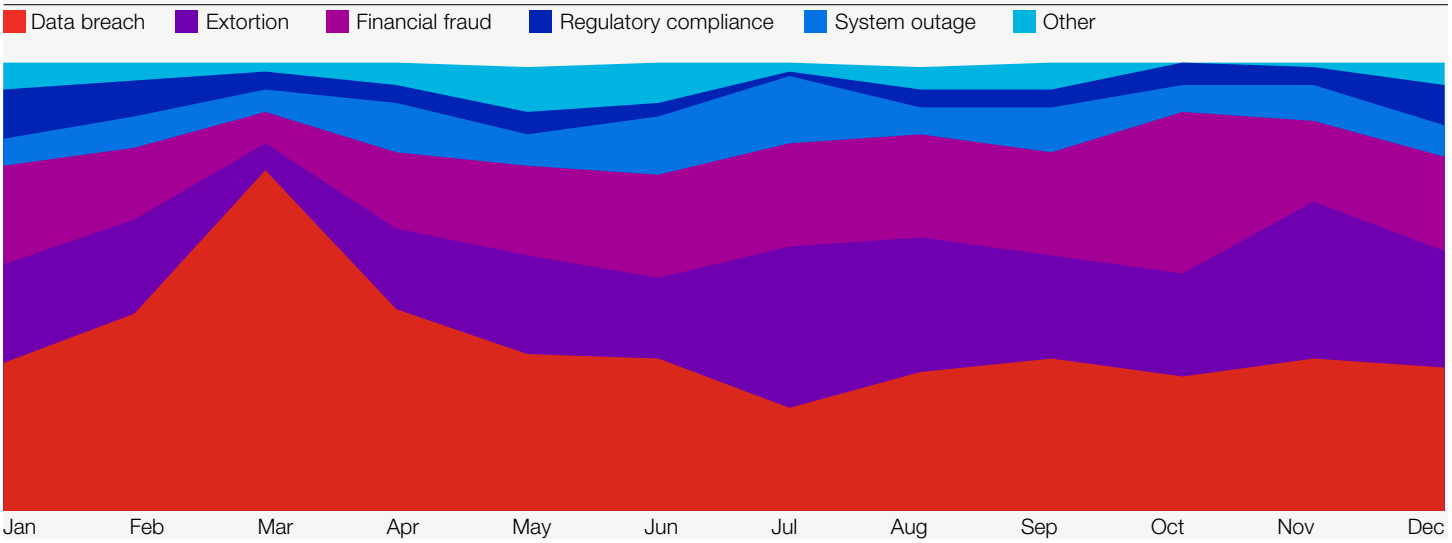


2021 claims count by impact
All Hiscox retail territories



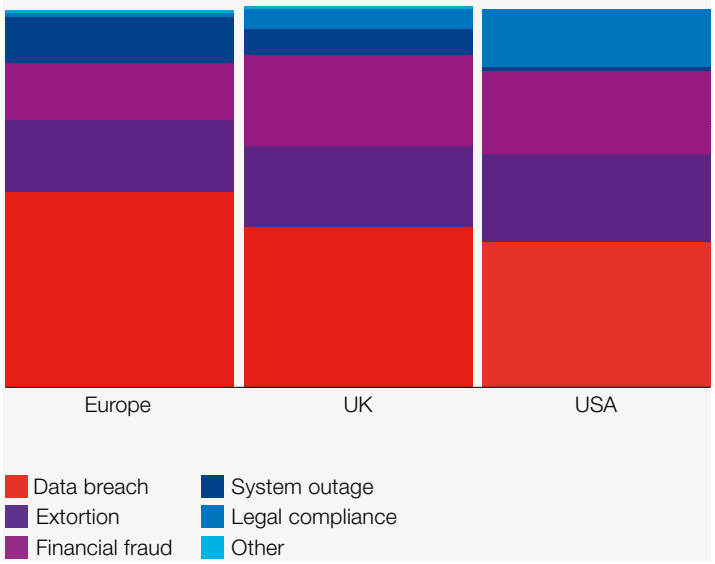
2021 saw an increase in data breach claims, with ransomware holding steady year on year.

2021 claims impact
All Hiscox retail territories



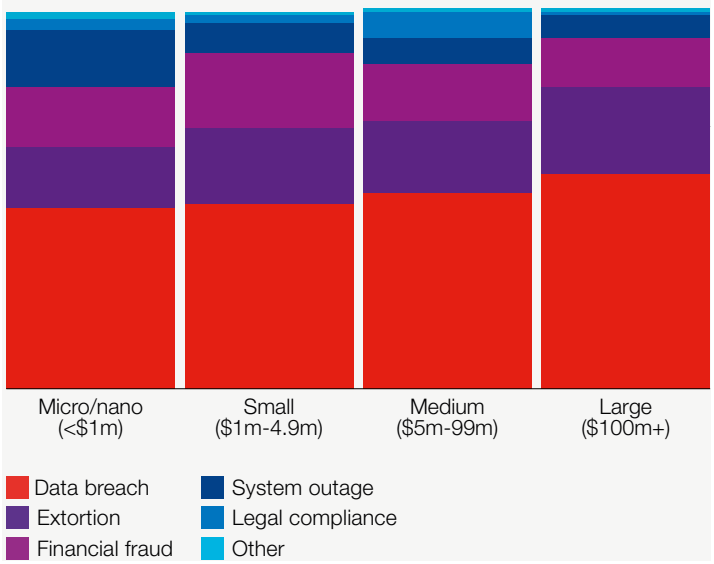
As noted previously, there was a significant increase in data breach claims in March 2021 due to the Microsoft Exchange incident.

2021 claims count by geography
All Hiscox retail territories



In 2021 data breaches were the predominant claim type in all our retail geographies.

2021 claims count by company size
All Hiscox retail territories



Across micro-, small-, and medium-sized businesses, there's very little difference between the types of attacks our customers faced.

Cyber in the news 2021

Not all newsworthy incidents affected Hiscox, but large supply chain losses have the potential to lead to a greater surge-event. 2021 was an important year for customers and carriers to understand the impact of core software vulnerabilities, as well as the importance of basic risk mitigation techniques.

	Cyber in the news*	Hiscox view
Q1	Microsoft Exchange – on 3 March 2021, cybersecurity and infrastructure security (CISA) partners observed active exploitation of vulnerabilities in Microsoft Exchange Server products.	The Exchange server hack, attributed to a group called Hafnium, impacted over 30,000 servers globally – this makes it one of the largest attacks in the last three years.
Q2	Colonial Pipeline – on 7 May 2021, America's largest refined products pipeline went offline after a hacking group called Darkside infiltrated it with ransomware, which led to fuel shortages across the East Coast.	Attacks such as this and the JBS foods ransomware attack brought supply chains into sharp focus, and led to a crackdown by the US government on ransomware gangs.
Q3	Kaseya – is a managed service provider (MSP) that provides IT solutions to more than 40,000 companies worldwide. In July 2021, Kaseya's incident response team reported a potential security incident involving software that would potentially affect both on-premises and SaaS clients.	Supply chain attacks such as this and the previous SolarWinds attack, reinforce the need to not only secure your network, but understand the security of your supply chain.
Q4	Apache Log4j – on 9 December 2021, a Log4j software component vulnerability was released, which has had an incalculable systemic risk due to the widespread use of Log4j library in millions of products or app components.	Even though very little damage was reported, this was a very pervasive vulnerability. It has shown the value of having a Software Bill of Materials (SBoM) – a complete inventory of software running in your estate, to be able to manage vulnerabilities like this.

*Note that claims incidents in the news are not explicitly Hiscox claims but provided as examples and time stamps using public information.

Top Hiscox claims trends

Data breach and cyber extortion were the top claim impacts in 2021, compared to data breach and financial fraud in 2020.

1 Extortion

Extortion continues to drive costs both last year and this year – 74% of 2021 incurred losses were due to extortion. The USA (43% of extortion losses) incurred the most expenses, followed by Europe (37%) and then the UK (20%). The top ransomware variants our insureds encountered were Conti, REvil, and Ryuk. Losses and severity of ransomware dropped towards the second half of the year, a trend not seen the previous year. This was likely due to the pressure applied by authorities, which drove threat actors to cause less disruption.

2 Data breach

Data breach was the most common claim, making up 34% of the total, but incurring only 10% of the losses. 39% of data breach claims were caused by Microsoft Exchange, but even so, losses decreased 70% from last year. The most common points of entry for data breach claims were system vulnerabilities and business email compromise (BEC). The UK led in BEC severity, followed by Europe, and then the USA.

3 Financial fraud

Overall, financial fraud losses decreased in 2020 by 35%, even though the number of claims increased by 37%. It accounted for just 6% of all Hiscox cyber losses in 2021. Social engineering was the leading cause of financial fraud, and 17% of those social engineering attacks led to BEC. 47% of the financial fraud claims came through Europe.

Real-life scenarios

Open ports lead to ransomware

Our insured had an open VPN port for their remote users. It was configured with the default password and did not require multi-factor authentication (MFA). After gaining administrative privileges from the compromised VPN account, the threat actor fully encrypted the company's servers. No ransom was paid, which was the insured's decision. Losses were incurred through repair and recreation of servers.

Business email compromise and financial fraud

An email account of one of our insured's clients was compromised. Our insured received fraudulent instructions from the client's email address, asking them to update the direct deposit information for one of their employee's payroll payments. Our insured's employee updated the information as requested, without a multi-step process to confirm. The payroll payment was deposited into the fraudster's bank account for two months before the client's employee noticed they had not been paid and alerted the insured. The bank was notified of the fraudulent transaction and recovered the payment.

Accidents can cost us

A data breach occurred when our insured's employee mistakenly sent a number of documents containing personally identifiable information (PII) to the wrong client. The client then sued our insured because the correspondence contained personal details including name, address, date of birth, etc. We assisted our insured in providing compensation to the client for the breach of their personal data.

Mitigate the risks

Demand your vendors comply

Due diligence on supply chain vendors is essential, especially if they process insured's data. We've seen attacks on software vulnerabilities and hosting services cause breaches for all the businesses that use these services. Solar Winds, Microsoft Exchange, Kaseya, and Log4j attacks should all make companies pause and take the time to audit the services and vendors they use.

Build a human firewall

Train employees to spot and manage phishing emails, as well as understand other cyber risks. Social engineering and BEC were key causes in data breach and financial fraud claims. Both points of entry can be managed through phishing tests and other employee training. Our people are the first line of defense against a cyber attack. Hiscox currently offers the Hiscox CyberClear Academy, a free cyber awareness training platform, to all of its cyber insurance customers.

Enable multi-factor authentication (MFA)

Microsoft Office 365 compromises continue to be the root cause of many BEC and financial fraud breaches. On all user accounts, but especially administrator accounts, MFA is a simple first-step towards security.

Test your back-up strategy

It's not enough to simply have frequent back-ups both online and offline. You need to ensure your back-up plan is tried and tested.

Patch and update frequently

Major vulnerabilities such as Microsoft Exchange and Log4j could have been prevented by updating the patch. Usually, patches will be released very quickly and it's important companies apply all recommended updates and patches to minimise risk and defend against an attack once a known vulnerability has been exploited.

Close all unnecessary open ports

Remote desktop protocol (RDP) was a key driver in ransomware attacks and ultimately data exfiltration last year. Hiscox drove awareness during our underwriting process and we've seen a decline in breaches caused by an open RDP port. Generally, incidents can be prevented by patching, disabling ports (unless necessary), and limiting port exposure to the internet. Ports which must remain open should be regularly monitored.

2022 watch list

Supply chain/invisible supply chain vulnerabilities

Next year we expect the supply chain attack trend will continue, and we see there being at least three distinct varieties:

i. a 'visible' supplier of yours (e.g. SolarWinds/Exchange) – a malicious actor exploits a known vendor/partner;
ii. an 'invisible' supplier (e.g. Log4j/Eternal blue) – where a third-party vendor/open source library that a vendor or you rely on is breached;
iii. you are targeted as part of a larger vendor's supply chain. We have seen a number of incidents whereby smaller (and less well funded) companies have been targeted as an easier method of entry into large businesses.

The hybrid working world is here to stay

We reported in our 2021 Hiscox Cyber Readiness Report that 41% of respondents had increased numbers of staff working remotely, a trend that continues as working practices, including hybrid working, evolves. Nearly one-fifth of businesses (18%) are adapting with new e-commerce channels. However, these changes were forced on businesses at very short notice, meaning they were not always planned, tested and secured with the rigour that they might have been under more normal times.

The Log4j vulnerability at the end of 2021 is a good example. If a company has had to invest in a new VPN solution it may not have sufficient in-house skills or experience to ensure that service is checked for the vulnerability and remediated in a timely fashion.

Ransomware evolves, but regulation starts to bite

2022 will see the continued cat and mouse fight between the ransomware gangs and defenders/law enforcement. Expect ransomware groups to morph and rebrand, as well as keep affiliates closer to minimise their chance of infiltration or compromise by competitors/ disgruntled affiliates. Ransomware techniques will no doubt evolve, perhaps with better tools to exfiltrate sensitive data for 'double extortion' attacks.

Law enforcement will continue offensive cyber operations against ransomware gangs, and companies will be forced to do a better job at segmenting networks, securing back-ups and improving their resiliency.

Regulators will continue to focus on crypto exchanges, putting pressure on them to make it more difficult for criminals to 'cash out' their illegal gains.

4 Activism moves online

2021 was another year in which a number of protest groups have taken direct action is response to the climate challenge and other socio-political issues the world is facing. The majority of this direct action has been physical events, ranging from protests to more intrusive action such as motorway blockades.

2022 could be the year we start to see protestors move online in a meaningful way.

5 Quantum computing

Quantum is gaining momentum with some analysts predicting that a quantum computing breakthrough is around the corner. We're not convinced that this will necessarily come true in 2022, but what is undeniably true is that headway is being made and quantum's time is definitely coming. The world needs to consider the implications of ubiquitous quantum computing soon, and plan for its arrival.

6 Cyber war and cyber operations

Continuing geopolitical conflict between the West and Russia has raised the potential for cyber attacks against western targets. Current assessments project that any Russian sponsored cyber attacks could be focused on critical national infrastructure and finance-related targets*. All businesses and their employees should remain extra vigilant, but companies in sectors such as telecommunications, energy, and financial services should be on high alert, as well as any companies who would use these services via their supply chain or a third party. The main threat from Russian elements is likely to be ransomware, with phishing emails against staff a critical enabler in launching successful ransomware attacks.

*The Cybersecurity Risks of an Escalating Russia-Ukraine Conflict (hbr.org).

Glossary

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.

Ex-employees/insider threats.
This includes disgruntled ex-employees or employees with bad intentions.

Financial theft.
Cyber crime involving the theft of money.

Human impact.
Unintentional actions or inactions by employees (negligence) that can result in a cyber incident. This includes spoofed emails, phishing, payment diversion fraud (PDF), accidental disclosure, etc.

Managed Service Providers (MSP)/third party.
Cyber incidents resulting from a third party or vendor.

Misconfiguration.
Incorrectly configuring certain technologies leading to a cyber incident.

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.

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 Ltd
Chesney House
96 Pitts Bay Road
Pembroke HM 08
Bermuda

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

22065 07/22