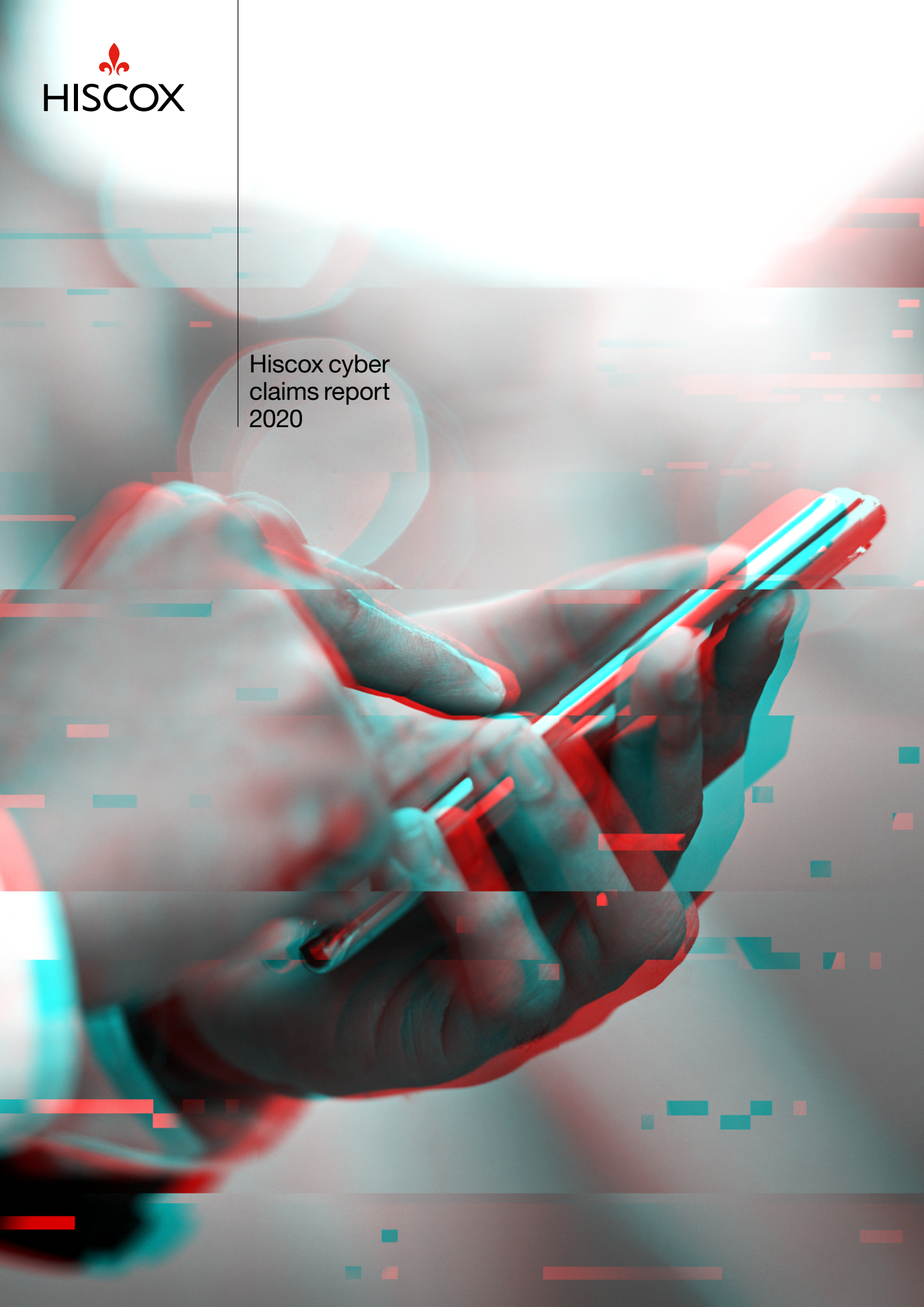




Hiscox cyber  
claims report  
2020



---

## Introduction

The year of 2020 was unlike anything in recent memory. As the world battled Covid-19, many businesses transitioned online, and risks shifted from physical security to cyber security.

Though cyber risk is not new, the overnight shift in business models led to an immediate demand for collaborative technologies, remote access, and the need for businesses to create an online store while physical stores were closed. But speed to market and security don't often go hand-in-hand. Many businesses didn't have the in-house expertise or time to set up proper governance and security monitoring for their new technology. Cyber risk didn't necessarily increase overnight, but it did shift based on the pace of business needs, which had implications later in the year.



**Gareth Wharton**  
Cyber CEO  
Hiscox

A handwritten signature in black ink that reads "Gareth Wharton".

Another major shift was in ransomware tactics. In early 2020, ransomware gangs were no longer simply locking data, which could be restored when good back-up practice was in place. They took cyber extortion and added data exfiltration, as well as distributed denial of service (DDoS) attacks to the mix. To stop gangs from publishing personally identifiable customer information or to get their ecommerce sites back online, companies had few options but to pay ransoms. Traditional, good back-up strategy was no longer a fool-proof fix against ransomware.

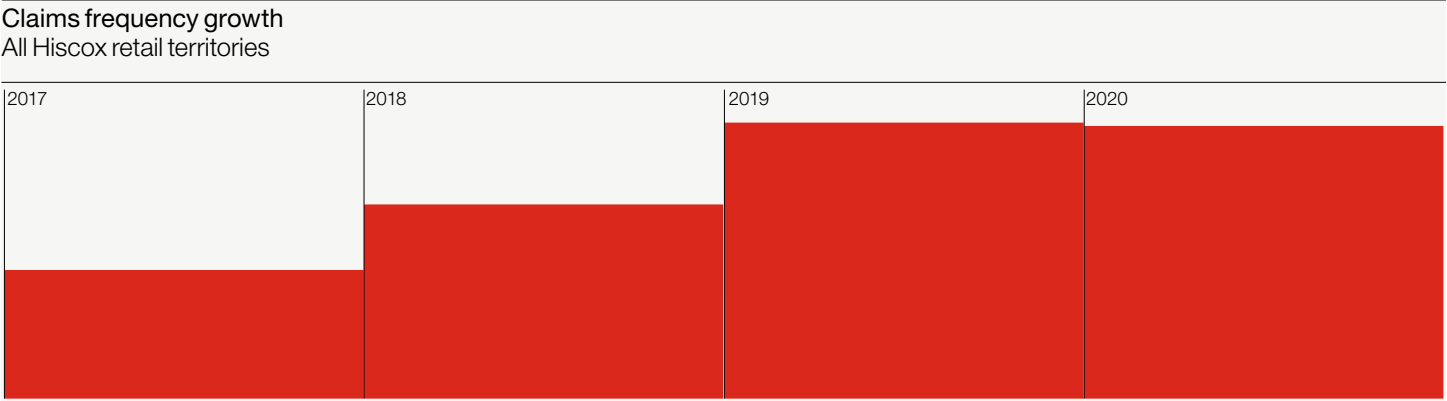
And we saw a continued trend in supply chain attacks, leading to additional breaches for those using certain vendors. Major news outlets highlighted the attacks of large service providers like Blackbaud and SolarWinds, illustrating the importance of monitoring cyber risk along your supply chain.

Claims across our Hiscox retail businesses in 2020 reflected the impacts of an overnight shift to remote working, as well as the need for continued vigilance against the ransomware challenge. Cyber training is as important as ever given that human error played a part in over half of Hiscox claims. Mitigating ransomware and data exfiltration could decrease the severity of costs and length of business interruption. Basic cyber security like multi-factor authentication, prompt patching of critical assets, and due-diligence with third-party vendors' security would all protect against the cyber challenges to come.

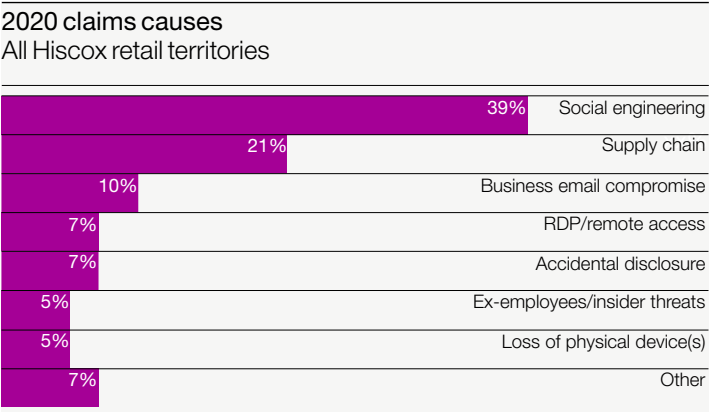
The overall shift in cyber security risk and headline-grabbing ransomware attacks made 2020 a challenging year for cyber; however, it also grew awareness for this constant, yet manageable risk. Basic cyber security measures are still the best road to cyber resilience and paired with a cyber insurance policy help a business mitigate, manage, and recover from an attack.

# Cyber claims by numbers

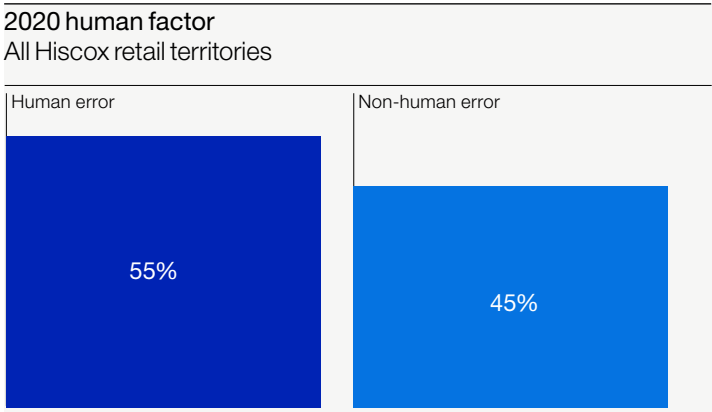
Claims causes illustrate the need for continued employee training.



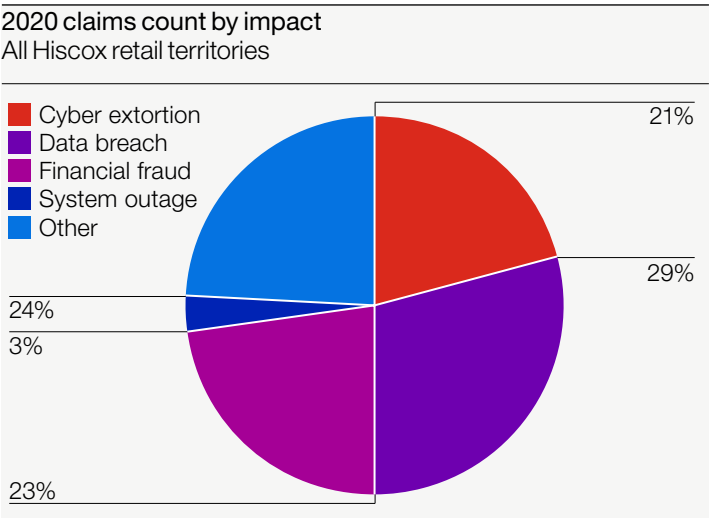
Claims frequency nearly doubled from 2017 to 2019.



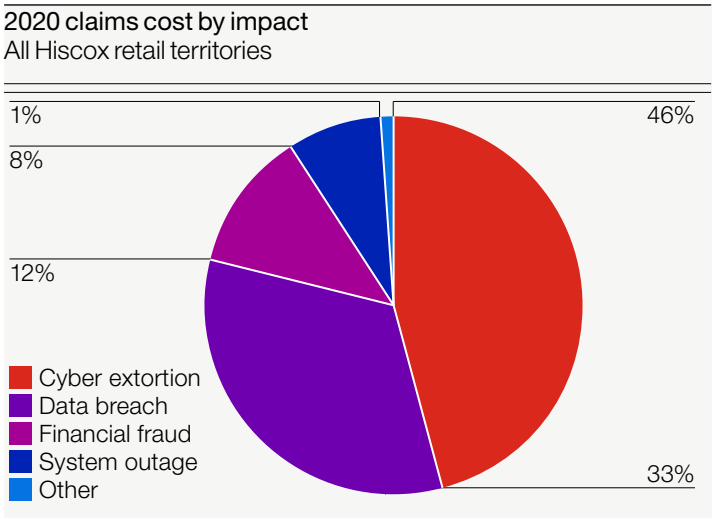
Social engineering\* and supply chain were top, stressing the importance of employee training and assessing vendor security, as well as your own.



Over 50% of claims were caused by accident or human error. Employee training is the number one way to manage this major human factor.



Most frequent claims in 2020 involved data breach, other\*\*, and financial fraud. Other, which includes vulnerabilities are often claims that require discovery, but no additional costs for breach notification.



Cyber extortion, combined with data breach are driving the costs of claims, due to ransomware and the evolving trend of doxing.

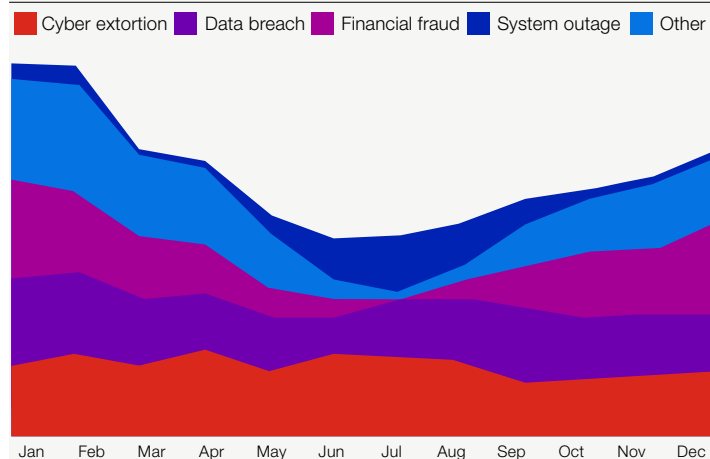
\*Social engineering includes incidents such as phishing, payment diversion fraud and pretexting.  
\*\*Other – this includes incidents such as telephone hacks, data destruction, cryptojacking and any other incidents that do not fall under the other impact types.

# Cyber claims by numbers

Data breaches grew as ransomware trends shifted.

2020 claims count over time (impact)

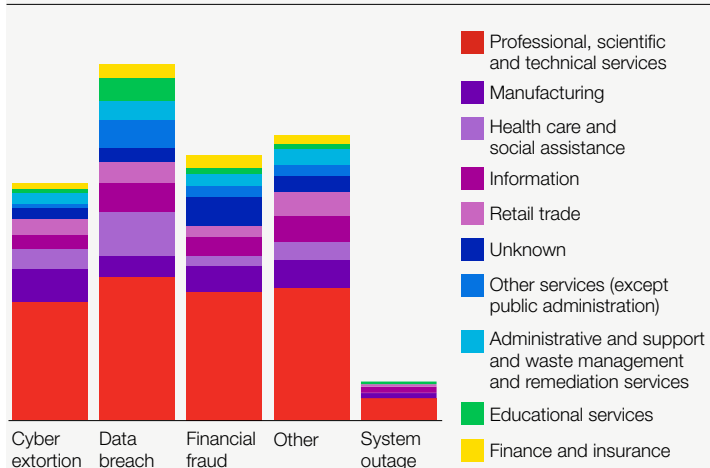
All Hiscox retail territories



Surge of cyber extortion in summer continued to be a challenge all year and likely to continue throughout 2021.

2020 claims count by industry (impact)

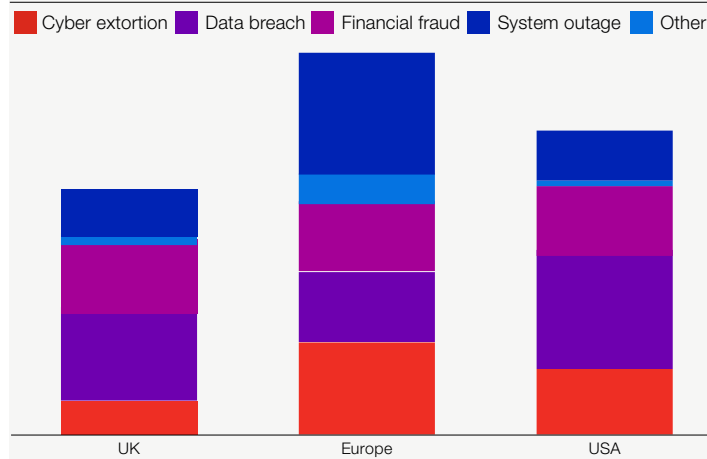
All Hiscox retail territories



Professional, scientific, and technical was by far the top industry targeted, followed by manufacturing and health care. Though affected industries reflects Hiscox customers, health care has been especially impacted given the pandemic.

2020 claims count by region (impact)

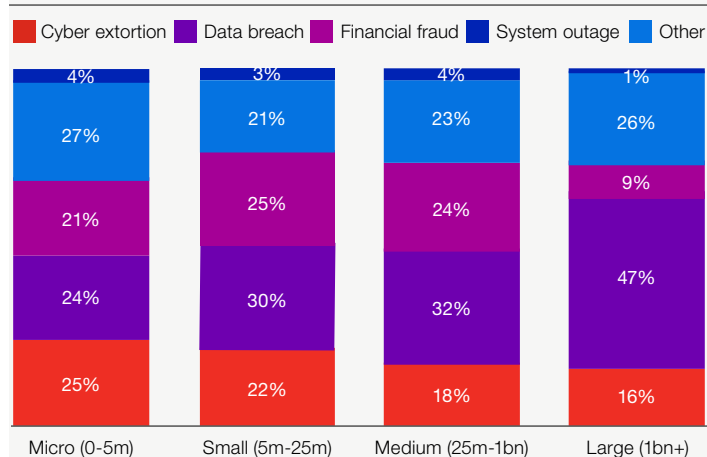
All Hiscox retail territories



Europe had the most notifications, but costs were highest in the USA. Early notification seems to be a common practice in Europe, which leads to shorter business interruption time and lower overall costs.

2020 claims impact type by size

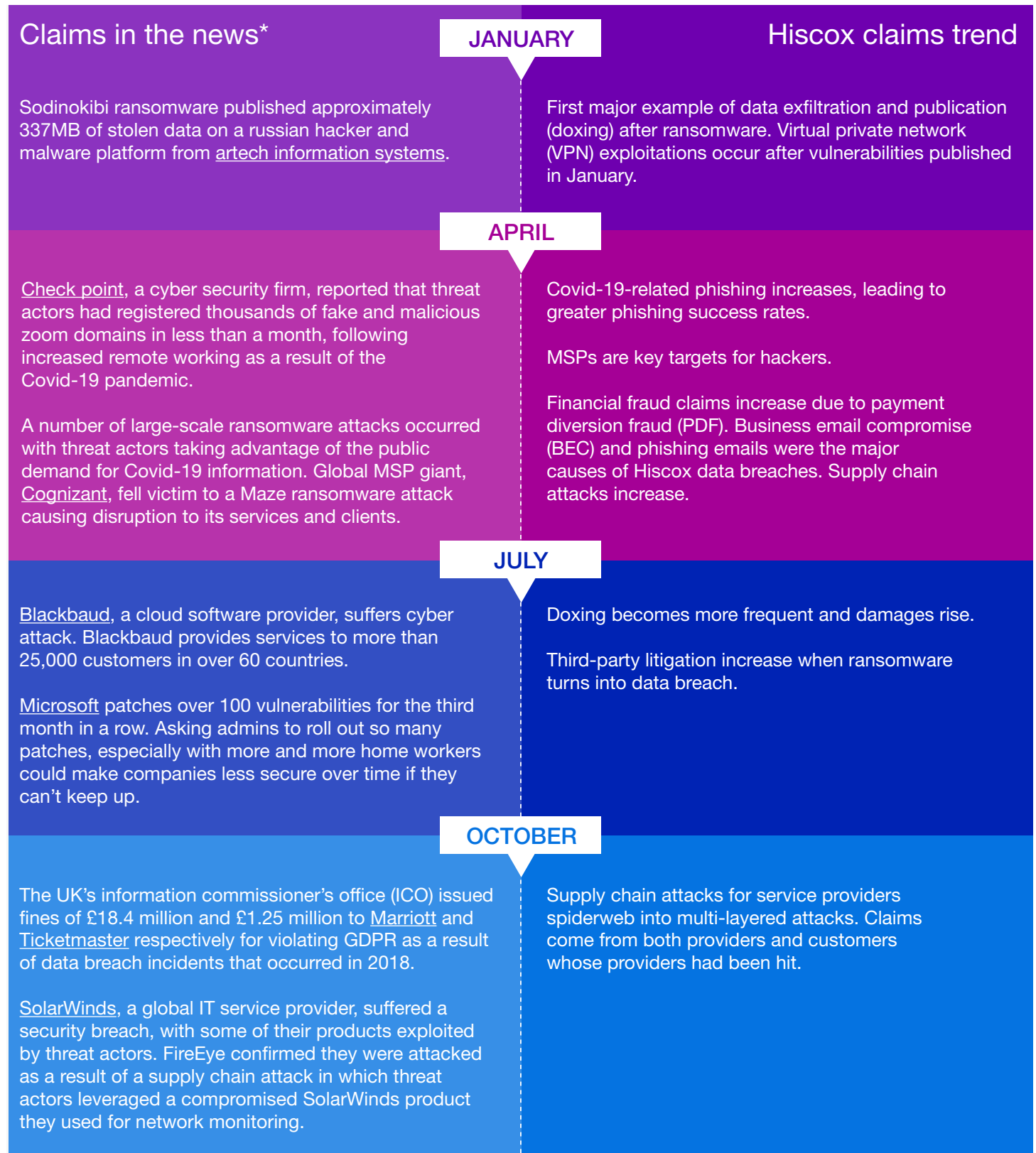
All Hiscox retail territories



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

# 2020 claims trends

Hiscox claims trends fell in line with many of the cyber incidents documented in the news throughout 2020.



\*Note that claims incidents in the news are not necessarily Hiscox claims but provided as examples and time stamps using public information (sources linked).


# 2020 claims trends

Key trends included VPN exploitation, Covid-19 phishing, supply chain risks, and ransomware.

## Virtual private network (VPN) exploitation

Security researchers reported security vulnerabilities in several VPN services being exploited in the wild. VPN devices need to be internet facing, which makes it easy for attackers to scan the internet for these vulnerabilities. These vulnerabilities gave attackers remote access to a network without login credentials. In all cases, attackers could then run their own code to access internal systems, exfiltrate data, install ransomware, and/or wipe devices. At least 15% of claims notified in January involved VPN vulnerabilities.

### Real-life scenario

Sector	Transportation	
Revenue	£100-500 million	
Claim cost	£250,000	
Incident	Insured is a public transport corporation that suffered a ransomware attack after threat actors exploited a recently published vulnerability in Citrix Netscaler, a well-know VPN solution. The threat actors also attempted to exfiltrate sensitive data but were unsuccessful.	
Resolution	Insured engaged the services of a non-Hiscox vendor and Hiscox supported with ICO notification and business interruption costs.	

## Covid-19 phishing continues

As part of efforts to manage the spread of coronavirus (Covid-19), many companies mandated or encouraged their employees to work from home. One of the top threat's businesses faced with their employees working remotely was coronavirus-themed phishing emails. Cyber criminals took advantage of the anxiety and thirst for information by sending out phishing emails with information on Covid-19 such as vaccines, tax refunds, preventive measures from the World Health Organisation etc.

### Real-life scenario

Sector	Manufacturing	
Revenue	€1-5 million	
Claim cost	€10,000	
Incident	Insured suffered a ransomware attack on one of their computers of the Ako/MedusaReborn variant. Unfortunately, back-ups were dated two months prior due to the fact that there was a blackout in the location where the network attached storage (NAS) was located during the lockdown. The restriction in movement resulted in the blackout.	


Resolution	Hiscox engaged our forensics vendors to carry out an investigation where the ransomware variant and mode of entry were determined. The insured was able to restore from back-ups, although there was some data loss as a result of the backdated NAS.
------------	---

## Supply chain attacks

There was a continued trend of supply-chain attacks throughout 2020. An attack on a software provider resulted in 22% of Hiscox data breach claims in Q3. With an increased number of ransomware attacks involving data exfiltration, companies can no longer rely on efficient back-ups to mitigate ransomware attacks.

In December, an IT service provider suffered a security breach as part of a large campaign, where their products were being exploited by threat actors. This triggered multiple claims notifications especially in the USA (17% of the USA claims were in December), and though there were no cyber attacks on the affected insureds, forensic costs to asses any potential damage were incurred.

### Real-life scenario

Sector	Charity	
Revenue	£1-5 million	
Claim cost	£10,000	
Incident	Insured is a charity providing small grants in the UK. The insured was informed that data relating to donors including names, contact details, and amounts donated, was impacted in a ransomware attack on it's vendor (data processor). In this incident, a large amount of data processed by the vendor on behalf of the clients was exfiltrated by the attacker. The vendor paid a ransom to them on the condition that the exfiltrated data was destroyed.	
Resolution	The insured engaged lawyers to advise them and notifications to around 2,000 data subjects were made. Hiscox covered all legal fees.	

# 2020 claims trends

## Ransomware evolution

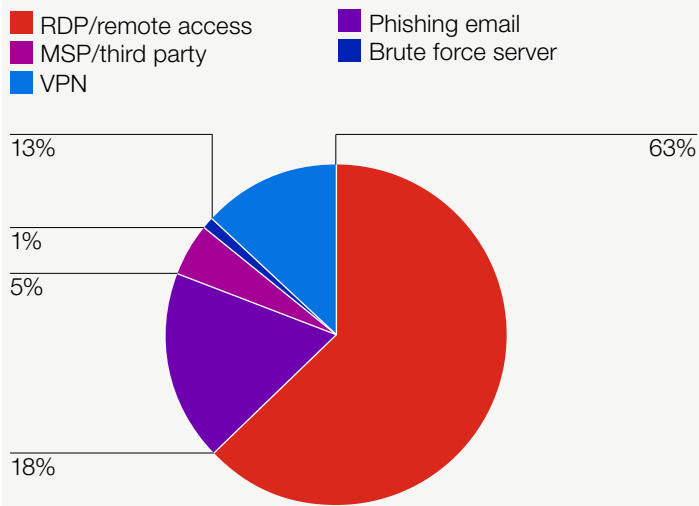
2020 saw an increase in the trend of ransomware attacks coupled with data exfiltration. Many ransomware gangs launched websites to either post stolen data to shame their victims, or auction stolen data. This was also reflected in Hiscox claims data where ransomware cases evolved from business interruption to data breach incidents. Hiscox also saw multiple data breach claims where the insured's vendors suffered such ransomware incidents, thereby affecting the insured's data.

## Real-life scenario

Sector	Media
Revenue	\$100-500 million
Claim cost	\$500,000
Incident	Insured is a media agency that suffered a ransomware attack where the threat actors exfiltrated the insureds data, including employee PII. This included names, home addresses, dates of birth, driver's license numbers, and SSNs of over 800 employees.
Resolution	The threat actors initially asked for a \$1.2 million ransom demand, which was negotiated down to prevent them from publically releasing stolen data.

## 2020 cyber extortion mode of entry

All Hiscox retail territories

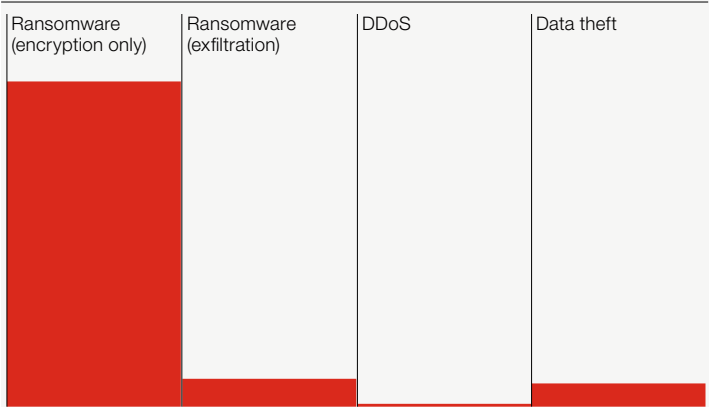


Remote Desktop Portal (RDP)\* remains the common point of entry in ransomware attacks. 63% of all ransomware claims of which we were able to determine the points of entry were via RDP open to the internet. Ransomware incidents evolved to include data exfiltration in many claims, thereby driving up the claims costs when you factor in regulator notification, credit monitoring etc.

\*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.

## 2020 cyber extortion type

All Hiscox retail territories



## London Market view

Though this report is focused on our retail business territories in the UK, USA, and Europe, the ransomware evolution has affected London Markets, as well. For companies over \$1 billion, ransomware claim frequency and severity rose sharply in 2020, and the tactic of doxing increased the time and cost of managing claims.

Pre November 2019, when ransomware was purely first party, the lifecycle of a claim really only depended on the speed with which the insured notified of a business interruption (BI) claim, in addition to any adjustment or negotiation around BI thereafter. Full recovery might have taken a year or less.

When doxing and data exfiltration entered the scene, not only were fees for breach notification and regulatory interaction added in, but potential for third-party litigation grew. Whether the litigation arose out of ransomware or a straight data breach, the time to close the claim might now be two to three years, and that's if litigation never goes to trial.

Claim frequency and the evolution of ransomware into doxing has increased severity and losses for companies over \$1 billion.

# Mitigate the risks

Cyber risks need to be managed. Help to decrease cyber risk by implementing some key mitigation measures.



## Build a human firewall

Train employees to spot and manage phishing emails, as well as understand other cyber risks. Employees 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 (O365) compromises continue to be the root cause of many BEC and PDF breaches for Hiscox in the USA and Europe. 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

VPN remains a common point 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. Ensure anti-malware software, IDS/IPS (intrusion detection/prevention software) etc. are 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

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. Ports which must remain open should be regularly monitored.



## Notify your insurance carrier early

Malware can be the first step to larger attacks with increased costs. The earlier you notify of a potential or actual claim, the faster your business can get back up and running. 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 – \$927,000 compared with \$492,000. As cases of data exfiltration continue to increase, early detection of malware is more important than ever to preventing a ransomware attack and potential doxing.



## Demand your vendors comply

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.

# 2021 watch list

So what's next? Certain trends are here to stay and businesses of all sizes must protect, stay vigilant, and build resilience.

1

## **SolarWinds fallout**

Immediate impacts and broad ramifications still unknown. Potential copycat attacks likely, leveraging software supply chains as targets. Build and deploy services have always been built for speed and convenience, not security. Be wary of exploitation of critical vulnerabilities in Microsoft products.

2

## **Evolution of ransomware**

Criminals are creative and innovative when it comes to putting pressure on victims to pay. Various attack vectors will be used in conjunction to cause further disruption – DDoS and doxing on top of ransomware. Open RDP ports and exploitation of remote access vulnerabilities will continue to be key avenues of entry for cyber criminals. Doxing poses a major threat to all businesses and the cyber insurance industry at large.

3

## **Continued Covid-19 threat**

Phishing campaigns will move from Covid-19 spread to vaccine information and sign-up. Attacks will likely target the Covid-19 response effort and corresponding industries and services – health care, local government, vaccine distributors, etc.

4

## **Legal landscape shifts**

Third-party and class action lawsuits will increase, along with GDPR fines as data breaches grow because of doxing and supply chain breaches. Given the pressure on ransomware, we'll likely see further government intervention and policy changes surrounding ransomware payments and prevention requirements.

5

## **New attack vectors**

We need to think as creatively as cyber criminals, anticipating their moves. Potential 'watch out' areas include: point of sale malware attacks, geomagnetic storms and other electromagnetic weapons, attacks on time protocols, and weaponized exploit kits from Nation States.



# 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 breach.**

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.

**Ex-employees/insider threats.**

This includes disgruntled ex-employees or employees with bad intentions.

**Financial fraud.**

Cyber crime involving the theft of money.

**Human impact.**

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

**Loss or theft of physical device.**

Losing a physical device containing insured's data.

**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](mailto:enquiries@hiscox.com)

[hiscoxgroup.com](http://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 US, 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](http://www.hiscoxgroup.com).