HISCOX
CYBERCLEAR®

Hiscox Global Cyber Claims Report 2022

Introduction

Early 2022 was marked by high anxiety over the Russia/Ukraine conflict, potential escalation, and what it meant for cyber risk across the globe. Almost a year on, many of those fears have not become reality.

Whether companies improved their risk management or ransomware groups have just been distracted, overall claims and ransomware specifically decreased from 2021. Compared to the average number of claims at Hiscox between 2018 and 2021, 2022 saw 18% less claims, despite policy count increasing.

Though the cyber risk is still present, it's shifted from large, mass attacks and ransoms that make headlines to smaller, simpler techniques. Smaller ransoms seem more likely to get paid and ransomware groups stay more anonymous by avoiding headlines and pressure from government agencies. For 2022, claims with recorded ransom demands, the average demand was 50% less than prior years. Ransomware occurred most frequently because of system vulnerabilities, followed by compromised credentials.

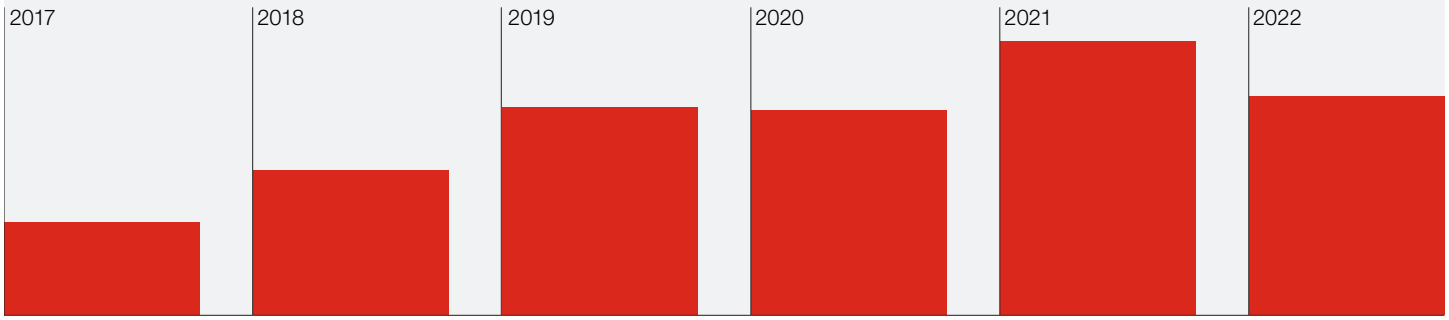
Less technically complex attacks like financial fraud through phishing campaigns have become the most common claim for Hiscox in 2022. This highlights the importance of continued cyber training for employees. Hiscox offers free cyber training for cyber customers through various partners across local markets. Education and prevention are key ways to mitigate some of the most common cyber incidents.

Looking ahead to 2023, we expect inflation and economic challenges to put continued pressure on cyber risk. Insider threats from disgruntled or desperate employees, were more frequent in 2022; resulting in a 160% increase in these types of claims, although this is from a small base. Additionally, though we may not get the big ransom headlines, ransomware groups will continue to attack, albeit more under the radar and focused on smaller mid-sized companies to avoid sanctions. On a more positive note, the growth of passwordless authentication for multi-factor authentication (MFA) would better protect companies and their employees from brute-force attacks or breaches using stolen credentials.

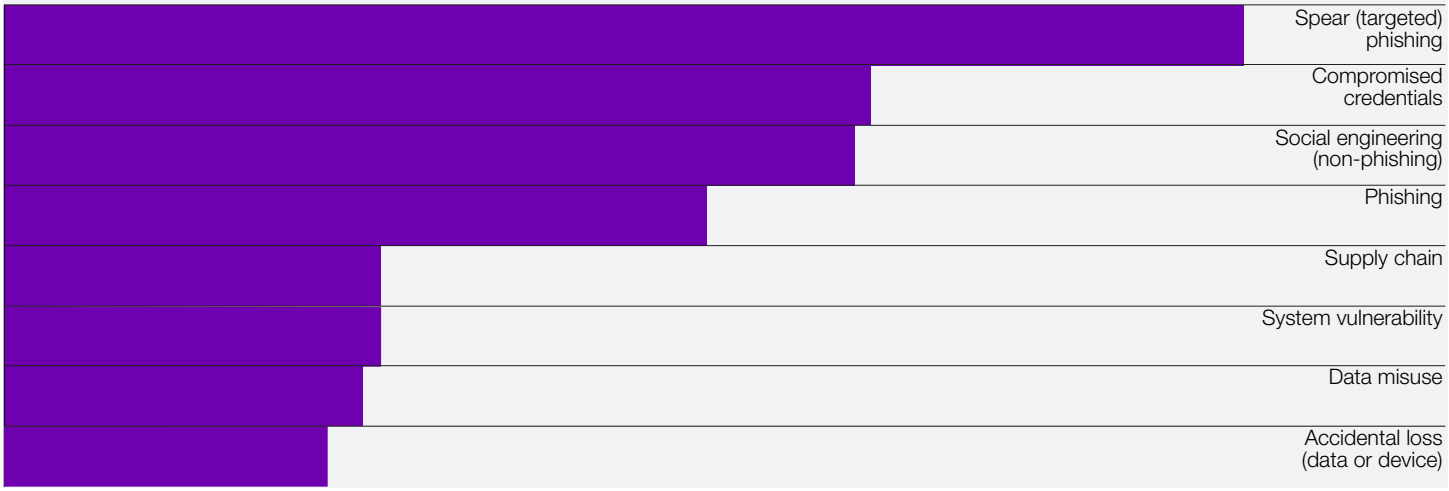
Gareth Wharton
Cyber CEO
Hiscox

Cyber claims by numbers

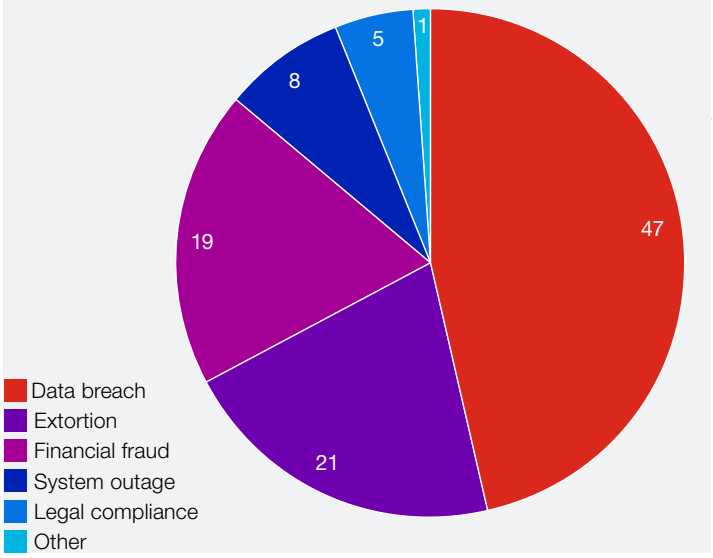
Claims frequency growth
All Hiscox retail territories



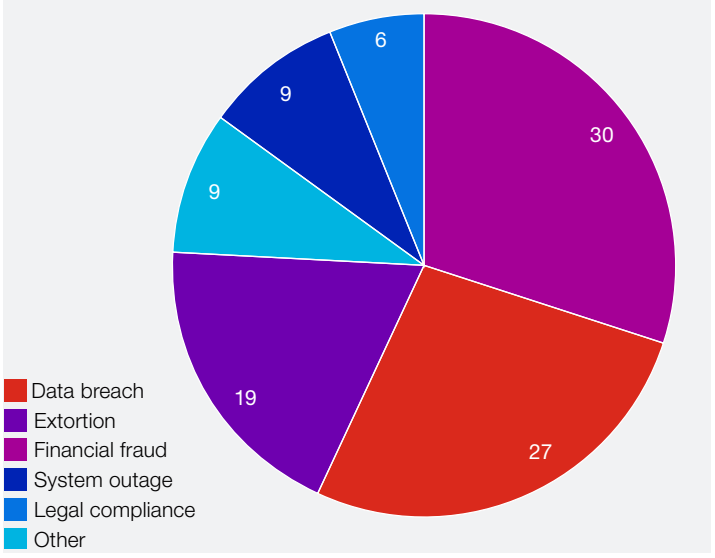
2022 claims causes
All Hiscox retail territories



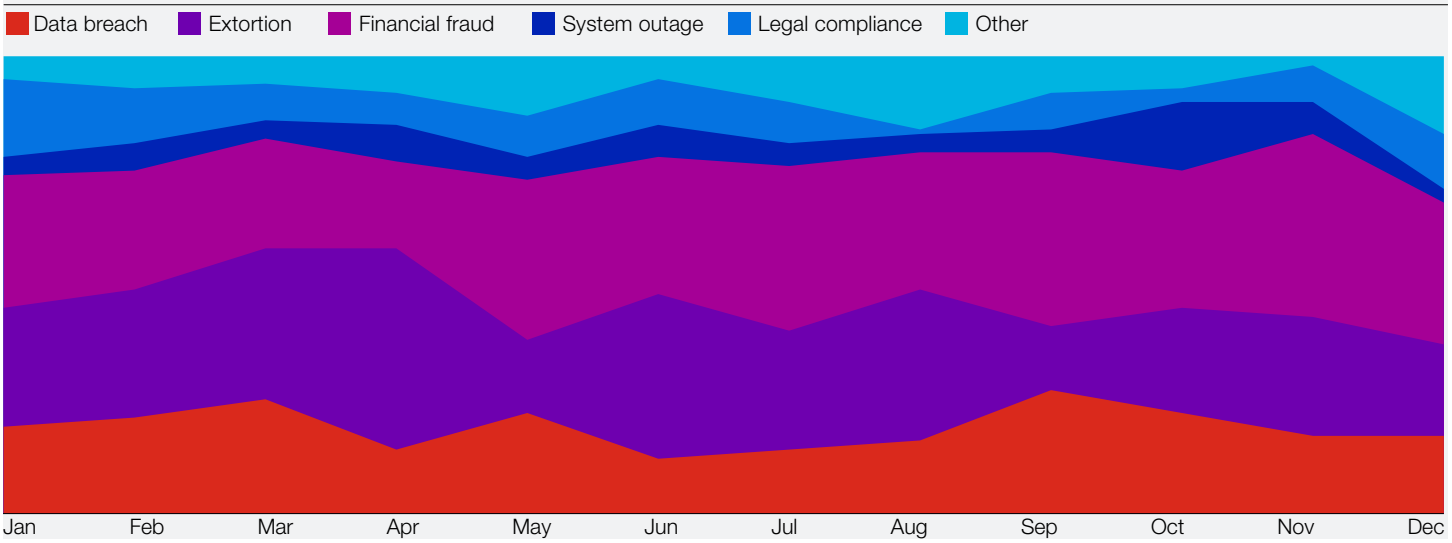
2021 claims count by impact (%)
All Hiscox retail territories



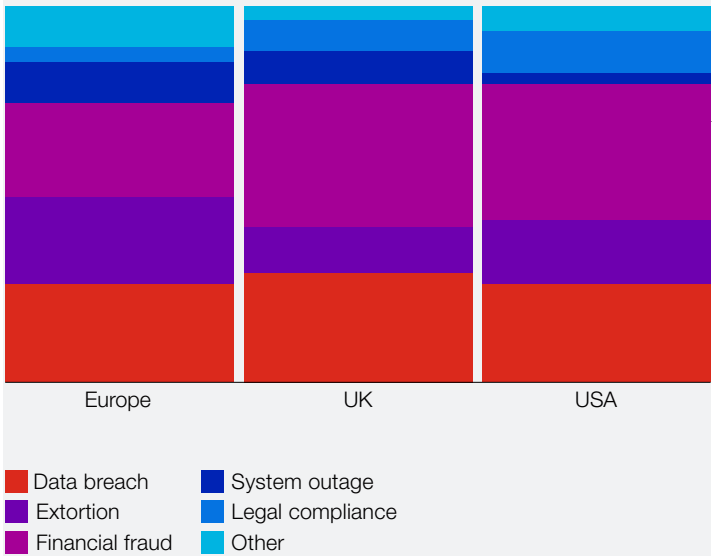
2022 claims count by impact (%)
All Hiscox retail territories



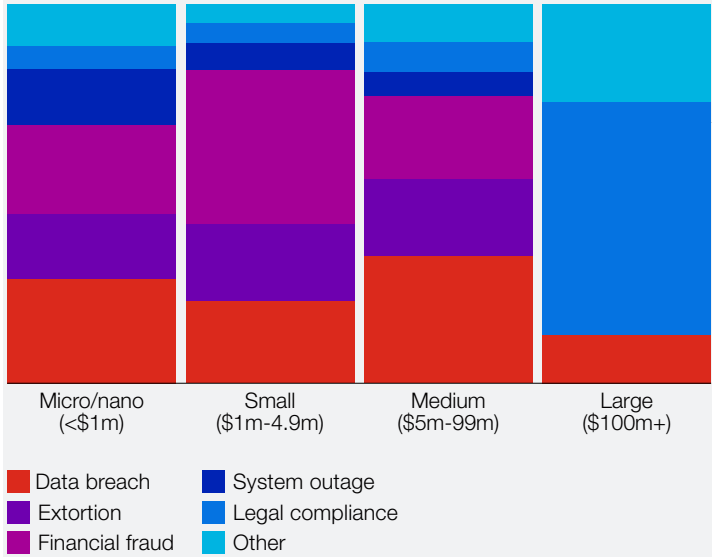
2022 claims impact
All Hiscox retail territories



2022 claims count by geography
All Hiscox retail territories



2022 claims count by company size
All Hiscox retail territories



Cyber in the news 2022

In 2022, after war broke out in Ukraine, businesses were on high alert for attacks, especially retaliatory attacks on the West. As the year went on, these risks seemed to decrease as other topics took over the headlines.

	Cyber in the news*	Hiscox view
Q1	The Russian invasion of Ukraine started on 24 February 2022. At this stage many ransomware groups began aligning with one country or the other, forming activist armies online. One notable group in particular, Conti, aligned with Russia.**	Many companies were on high alert for any types of retaliatory attacks by Russia. Hiscox assessed risk and ran table-top exercises with ourselves and clients to help companies feel prepared.
Q2	Apple, Google, and Microsoft announced plans to expand support for a common passwordless sign-in standard created by the FIDO Alliance and the World Wide Web Consortium. The new standard will provide websites and apps with the ability to offer an end-to-end passwordless option.***	We require and promote the use of multi-factor authentication (MFA) for our customers and their admin accounts, but not all MFA is equal. Password-only authentication is one of the biggest security problems on the web. The mandating of MFA by mainstream services will continue to help make accounts safer from both stolen credentials and brute-force attacks.
Q3	Shifts in ransomware techniques focus on the speed of encryption. A growing number of ransomware groups are adopting intermittent encryption, which means only parts of the targeted files are encrypted. This takes less time, but still renders data unrecoverable. Rather than encrypting data, some hackers are opting to outright destroy the data. Eliminating the stage of encryption makes the process faster and less complex and reduces the risk of not getting the full payout.	The number of ransomware incidents were down 46% for 2022 Hiscox claims. There was a pronounced reduction in maturity from almost all ransomware gangs due partly to the disappearance of gangs like REvil, Hive, Darkside, Blackmatter, Conti, etc. In 2022, the number of unique groups was up 45% and consisted more of lesser known gangs. There was a small shift in the techniques used to encrypt, exfiltrate or destroy data. Likely due to the variance of smaller, newer gangs introducing newer techniques.
Q4	ChatGPT was released by artificial intelligence R&D firm OpenAI in November 2022 and quickly amassed over a million users. The chatbot answers questions given to it in natural language by trawling vast volumes of data across the internet. However, its lack of moderation could be used for more nefarious purposes like building malware. It is clear ChatGPT may set the skill bar at ground level for wannabe cyber criminals.	Though claims were down in 2022, this does not mean cyber risk is not present. As new technology comes out like ChatGPT, building malware becomes more accessible to the masses. If ransomware-as-a-service (RaaS) changed the game over the last few years, this type of technology is one to keep an eye on. Continued cyber risk management and mitigation is essential.

*Claims incidents in the news are not Hiscox claims, but are provided as examples and time stamps using public information.
**scmagazine.com/news/ransomware/conti-ransomware-group-announces-support-for-russian-invasion-of-ukraine-threatens-retaliation
***wired.com/story/fido-alliance-passwordless-login-browser-support/

Top Hiscox claims trends

Financial fraud and data breach were the top claim impacts in 2022 compared to data breach and cyber extortion, which took the top spots in 2021.

1 Extortion

Extortion continues to be the main driver of costs this year and last – 74% of 2021 incurred losses were extortion, 70% of 2022 incurred losses were extortion. The top ransomware variants our insureds encountered were Lockbit, Blackcat, Hive and Conti. In comparison to 2021, the number of ransomware incidents was down 46%. Both the UK and USA saw a 56% decrease each in the count of extortion claims, Europe saw a 17% fall in the count of extortion claims.

2 Financial fraud

Financial fraud was the most common claim, making up 29% of all claims, although at only 11% of all losses. There was a sharp increase in the number of claims, where in 2021 financial fraud made up 19% of claims, in 2022 it was 29%. Spear phishing was the leading cause of financial fraud, equaling 31% of losses, followed by entry using compromised credentials or non-phishing social engineering, which incurred 28% and 22% respectively of financial fraud losses.

3 Data breach

After a surge in data breaches in 2021, due to the Microsoft Exchange vulnerability, breaches were 47% of all Hiscox cyber claims. In 2022, this leveled out to 20% of the total claims and only 11% of incurred losses. 20% of data breach losses were due to system vulnerabilities, followed by entry using compromised credentials and insider attacks at 10% and 9% of data breach losses respectively.

Real-life scenarios

Extortion

Our insured received an email from the ransomware gang 'Karakurt', stating they had exfiltrated over 1TB of the insured's data. The email contained a list of files they had stolen but did not state a ransom demand. No encryption took place on the insureds systems. The 'Karakurt' group was not engaged. Losses were incurred in forensics to determine the initial entry point and review what data was stolen. There was no business interruption as there was no system outage due to Karakurt's M.O. of only exfiltratrating data.

Financial fraud

An email account of one of our insureds was compromised. The threat actor set up rules in the victim's mailbox to duplicate all emails sent and received to another email owned by the threat actor. Using the stolen emails as a template, they altered invoices sent to a customer with different bank details. Under the pretence that the victim had mistakenly put in the wrong bank details, the hacker sent off the 'corrected' invoice to the customer. This resulted in multiple legitimate payments being diverted to the threat actor's bank account.

Data breach

Our insured terminated an IT employee. Thereafter, the insured started to notice that there was suspicious activity on the network. There were documents being moved and sent out. Investigations revealed the former employee was accessing the network remotely and either sending documents to himself or trying to encrypt them. We assisted the insured in forensic investigations to determine what data was breached and a subsequent review of the data. As no personal data was breached, a personal data notification was not required.

Mitigate the risks

Demand vendors comply and patch, patch, patch

Due diligence on supply chain vendors is essential, especially if they process an insured's data. We've seen attacks on software vulnerabilities and hosting services cause breaches for all the businesses that use these services. Though this was especially prominent in 2021, in 2022, we continued to see vulnerabilities exposed in software services used across a wide range of businesses. Companies should pause and take the time to audit the vendors and patch/update the services they use. Usually, patches will be released quickly and it's important companies apply all recommended updates and patches to decrease risk and defend against an attack once a known vulnerability has been exploited.

Build a human firewall

Train employees to spot and manage phishing emails, as well as understand other cyber risks. Social engineering and business email compromise (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 defence against a cyber attack. Hiscox currently offers free cyber awareness training platform options to all its small business cyber insurance customers.

Enable multi-factor authentication (MFA)

Microsoft Office 365 compromises continue to be the root cause of many business email compromises and financial fraud breaches. On all user accounts, but especially administrator accounts, MFA is a simple first-step towards security. As passwordless options continue to grow, investigate how to improve simple MFA options with more secure biometric and passwordless features.

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.

Close all unnecessary open ports

Remote desktop protocol (RDP) was a key driver in ransomware attacks and ultimately data exfiltration in 2021. 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.

Big business update

For larger companies with customers over 20,000 employees, claims volumes for cyber incidents were lower than anticipated in 2022. The war between Russia and Ukraine appears to have disrupted several threat groups earlier in the year, resulting in fewer successful attacks. Anecdotally, IT forensic and incident response specialist lawyers saw similar reductions, reporting volumes down more than 25% on anticipated levels. That trend at the start of 2022 has now started to reverse as cyber attack numbers picked back up at the end of year.

Meta pixel and wrongful data collection claims are a growing trend. Plaintiff firms are using various legislation outside of its intended purpose to seek settlement arrangements. Wire tapping laws and video privacy protection acts, for example, are being used to assert class action claims in the USA. Expect data protection claims to continue to rise in volume and severity throughout 2023.

Regulators appear to be flexing their muscles and moving to use the regulatory powers given to them in legislation over the past few years. Large settlements and proposed fines for investigations that commenced as early as 2018 are moving toward public announcement. Expect this to be a growing trend in 2023 and beyond. Coverage for fines will depend on wordings and applicable jurisdictions.

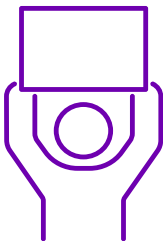
2023 watch list

Insider threats

In 2022, households and companies across the world were witnesses to elevated inflation, the subsequent interest rate rises, crippled supply chains, reduced economic activity and countless other problems. This is expected to continue throughout 2023, putting pressure on people and businesses. We expect insider cyber attacks to rise due to these factors, which have in turn made the following motivations more profound:

- financial motivation:
  when employees struggle to pay their bills, they are more driven to take risks for financial compensation. This could be the corruption of employees by criminal gangs, through bribes in exchange for intellectual property, remote access, credentials and more. We also expect financial fraud to rise as employees see more reasons to commit financially motivated crimes;
- disgruntled employee:
  with organisations now making large numbers of staff redundant and wages not meeting inflation, some employees may decide to exfiltrate company data or, in more extreme cases, delete data. Decreased morale will likely lead to more incidents due to negligence.

Attacks driven by activism



The Ukraine/Russia war has been fought on multiple fronts. One of these is through cyber warfare. Pre-war, Russia was seen as a cyber force to be reckoned with, although they have yet to achieve their high expectations. On the other side, Ukraine amassed an activist army consisting of 210,000 members, calling themselves the 'IT Army of Ukraine'. Although the IT army's cause is noble, it stands as a bad precedent for future activists. It raises the question: where will this army set their sights after the war?

If this is deemed as acceptable, where do we draw the line morally when it comes to other forms of activism? In 2022, for example, climate change protests became more frequent and dramatic. We expect tensions to rise in 2023, with an increased possibility that activists will resort to cyber attacks.

Ransomware gangs fracture

In 2021, ransomware were higher than previous years, resulting in global and local government authorities applying direct pressure to notorious ransomware groups. Perhaps related to this pressure, ransomware attacks did decline in certain parts of the world in 2022. In circumstances where ransomware did occur, companies refused to pay or were restricted from paying ransoms to many of these large, sanctioned entities. Simultaneously, ransomware group affiliates didn't want to work with any groups western intelligence agencies were targeting. Infamy doesn't necessarily lead to more successful cyber attacks.

For prolonged success, anonymity is the best way to evade authorities. When authorities get close to disabling a notorious ransomware group, they often break up into smaller, niche groups under different aliases and shift their targets. We expect this pattern to continue as groups see less benefit from infamy and more stability in smaller, clandestine operations that focus on specific industries or geographies. As part of this initiative, the headline-grabbing high ransom demands that bring unwanted attention from authorities have decreased in the last year, as well. In 2023, we expect continued lower demands and less frequent attacks, as fractured groups command fewer resources and attempt to stay under the radar.

4 Passwordless authentication

As organisations mature it becomes clear that password authentication alone is inadequate. The adoption rate of multi-factor authentication (MFA) has increased greatly, with MFA becoming a fundamental requirement for protecting remote services and online accounts. Mid-2022 saw Apple, Microsoft and Google commit to expanded support for FIDO standards in order to accelerate availability of passwordless sign-ins.

We see passwordless sign-ins as the next generation of authentication. Adoption of it by the three big tech companies will accelerate adoption as many organisations rely on their technology. With biometrics built into all modern devices designed by these companies, users can authenticate with their face, fingerprint, etc. Biometrics are far harder to phish and require physical access to the device, which authenticates the biometric and subsequently authenticates the session. We foresee further adoption of passwordless authentication in 2023 due to its ease of use and improved security.

5 Cable cutting

Cyber security is often fixated on digital, although there is and will always be the need for physical infrastructure to support the world's internet connection. Recently, the fragility of the fibre-optic cabling between countries has become more alarming. These submarine cables are a bottleneck for all internet communications around the world and any disruption could be extremely detrimental to daily life and business function.

In 2022, there were multiple attacks on these cables. All incidents were under suspicious circumstances. No one has been found responsible. Attacks like these will likely continue, as they are easy targets and highly valuable. Whether it is hostile nation-states targeting countries' internet connectivity, or activists targeting internet infrastructure is unknown.

6 Rolling blackouts

With the Russia/Ukraine war's effect on the world's energy supply chains, governments warned of the possibility of blackouts. In 2023, we could see these blackouts if energy supply struggles to meet demand. What would be the impacts in the cyber and security world? Data centres could see loss of power(although we expect governments to prioritise this infrastructure); remote work is most likely to be affected; companies may also struggle to maintain consistent power at their offices.

*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

22385 05/23