HISCOX

CYBERCLEAR®

Hiscox Global Cyber Claims Report 2023

Contents

01 Introduction
02 Cyber claims by numbers
04 Cyber in the news 2023
05 Top Hiscox claims trends
06 Mitigate the risks
06 Big business update
07 2024 watch list
09 Glossary

Introduction

Eddie Lamb
Chief Information Security Officer
Hiscox

Without doubt, the single most prominent cyber-related threat businesses face right now originates from organised crime groups, and the nature of the risk continues to evolve.

While these groups previously relied on ransomware attacks to monetise their hacking activities, advances in cybersecurity mean that businesses have become less vulnerable to this type of cyber extortion. Modern cyber defences are often capable of preventing computers from being infected with ransomware, and also enabling the rapid recovery from an infection– both of which are effective counter-measures to this form of extortion. That's not to say the threat from ransomware has been eradicated, but we know that this tactic has lost favour with organised crime because the likelihood of successfully extorting a victim has significantly declined over the last 24 months. Both frequency and severity of these attacks are in decline, with the average ransom demands in 2023 being 77% lower than seen in previous years.

As a consequence, organised crime has evolved its tactics and now focuses more keenly on the theft of sensitive data. In these cases, an extortion demand is typically made to the victim – a ransom of sorts in return for the data being kept out of the public domain. Extortion demands are based on the perceived damage that disclosure of the data could have on business operations and reputation. This is a cunning new tactic that is proving lucrative, and is likely to persist for the foreseeable future.

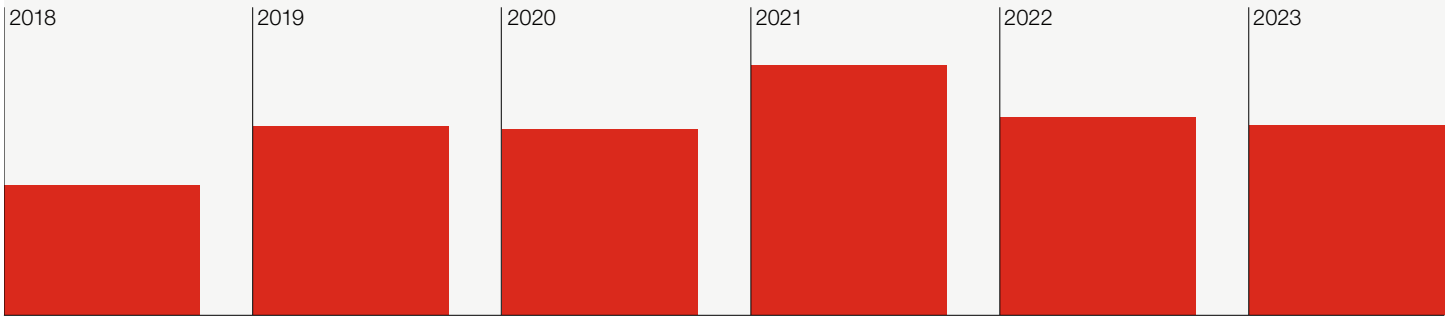
While the use of Artificial Intelligence (AI) currently dominates much of the media reporting on cyber threats, with much speculation that AI is actively being used to commit cyber crime at scale, our own claims experience sees little evidence of this yet. That is not to say that AI isn't being used – after all, it is intended to imitate human behaviour – but any conclusive evidence remains hard to find. One area we are confident that AI is being used in is in the analysis of stolen data to help identify information that can be used to support an extortion demand.

Another area where AI is emerging as a preferred tool is in financial fraud, with AI increasingly being used for impersonation in cases of payment diversion fraud – that is, where a victim is duped into transferring funds to a criminally operated bank account. Often these attacks are performed over phone and email, specifically targeting invoices being paid through the supply chain.

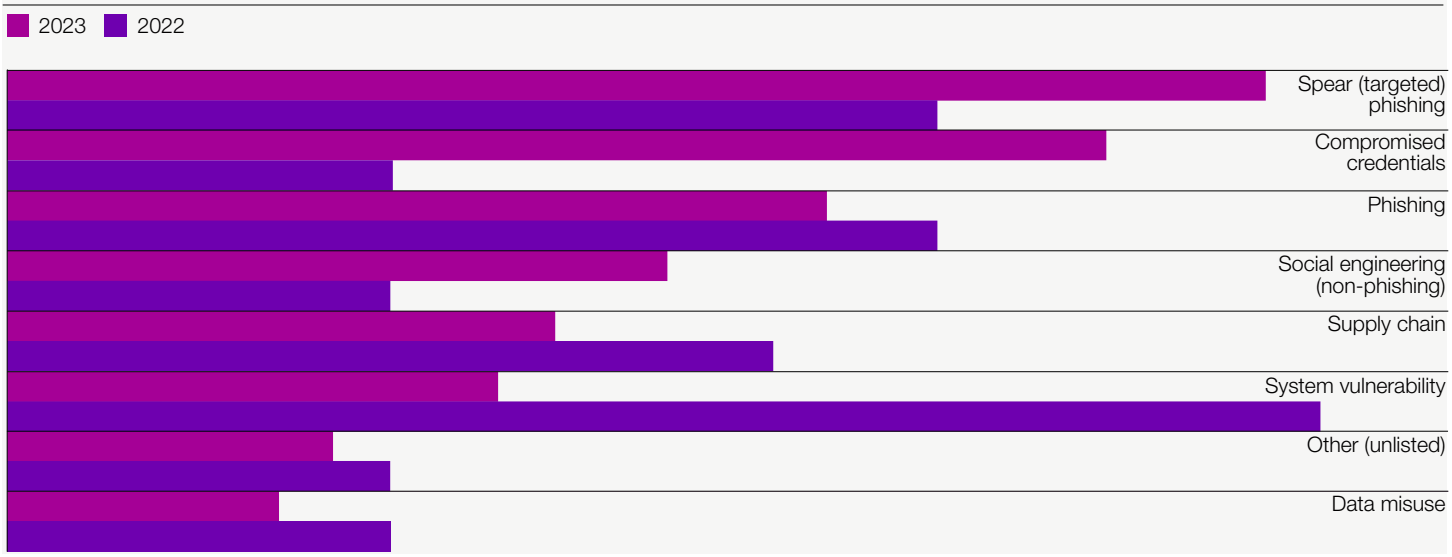
As we look ahead, we continue to see geopolitical instability, with periods of political and economic uncertainty often leading to increased cyber risk as new tactics and advanced cyber weapons are borne. A good example of this is the emergence of detection avoidant malware that seeks to overcome some of our current generation of malware defences. We should expect to see continued development of this criminal capability, which is why it remains vital to continually evolve our defences and stay one step ahead of the threat.

Cyber claims by numbers

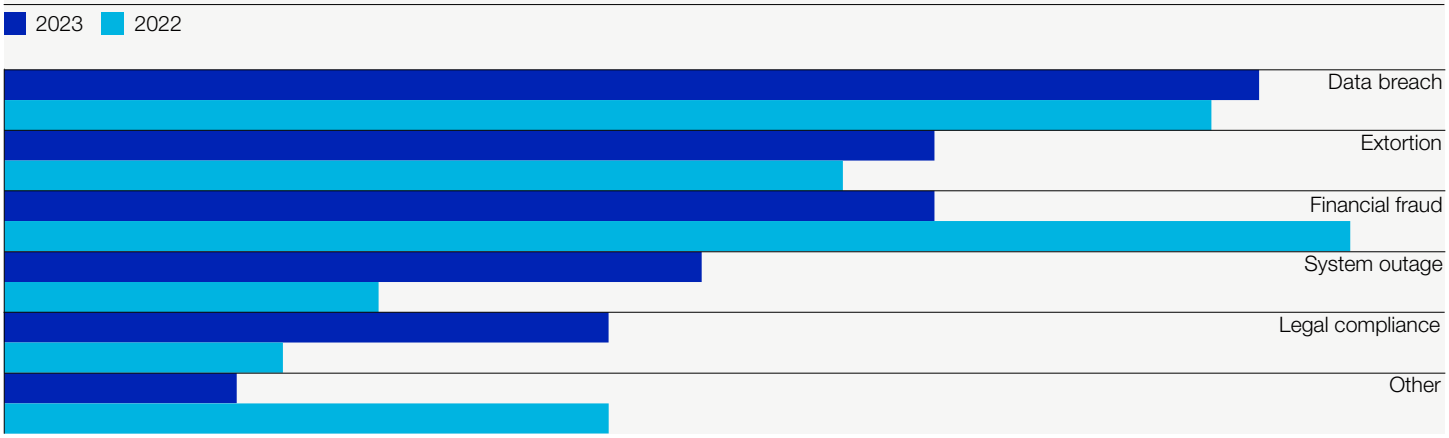
Claims frequency growth
All Hiscox retail territories



2022–2023 claims causes
All Hiscox retail territories

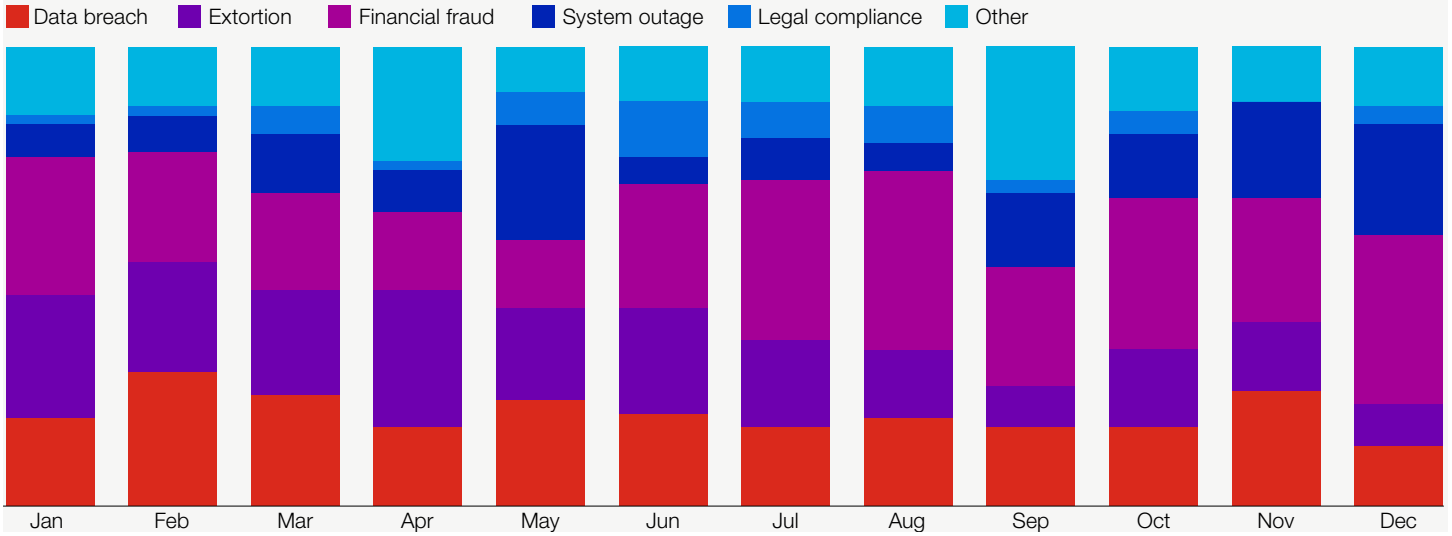


2022–2023 claims count by impact (%)
All Hiscox retail territories

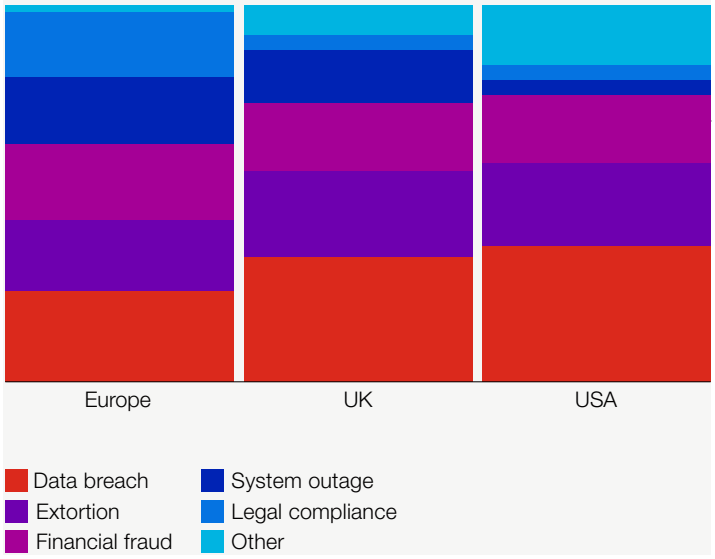


Cyber claims by numbers (cont.)

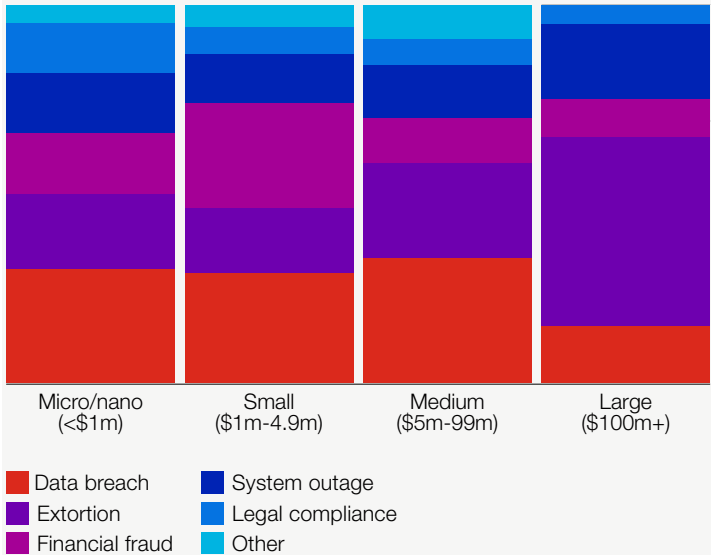
2023 claims impact over time
All Hiscox retail territories



2023 claims count by geography
All Hiscox retail territories



2023 claims count by company size
All Hiscox retail territories



Cyber in the news 2023

Several significant events in 2023 impacted businesses, including economic struggles and international conflicts. The cyber security field also saw numerous stories that significantly affected businesses, shaping the dynamics of how we protect ourselves.

	Cyber in the news*	Hiscox view
Q1	The FBI secretly hacked and disrupted the ransomware group Hive, preventing them from collecting over $130 million from 300+ victims. The undercover operation, which began in July 2022, went undetected until January 2023.	In 2022, Hive was a prolific group, they were our third most active group. This also follows the disappearance of Conti and several other smaller groups. With these groups no longer active we can look forward to a reduced threat and safer environment for businesses.
Q2	In March 2023, NCC Group recorded 459 ransomware attacks, the highest in three years, up 91% from February and 62% from March 2022. The surge was driven by the exploitation of CVE-2023-0669 in Fortras GoAnywhere MFT, primarily by the Clop ransomware gang, affecting 130 companies. Other active groups included Royal, BlackCat, and Medusa.	Following 2022's unexpected decline in ransomware incidents, we anticipated a subsequent rise. However, contrary to our expectations, the frequency of ransomware claims remained stable. The increase in reported incidents, as highlighted by the NCC Group, can primarily be attributed to the GoAnywhere 0-day vulnerability. Fortunately, our insured clients were largely unaffected by this 0-day exploit.
Q3	British authorities caution against rapid adoption of AI-driven chatbots due to security risks. The National Cyber Security Centre (NCSC) warns that large language models (LLMs) can be manipulated to perform harmful actions, such as unauthorised transactions via prompt injection attacks. The NCSC advises treating LLMs as experimental software, avoiding their use in customer transactions, and implementing robust cybersecurity measures to mitigate emerging risks associated with AI chatbots.	Artificial Intelligence (AI) is not just a passing trend; it is poised to become an integral part of our future. We welcome its potential to significantly boost productivity by automating everyday tasks, thus enabling employees to concentrate on more critical and creative aspects of their work. However, it is crucial for organisations to exercise caution when implementing AI systems. The potential security implications must be carefully considered and addressed to ensure a safe and effective integration.
Q4	In early December, the BlackCat group, also known as AlphV, experienced a dark web outage, followed by the FBI seizing their pages. Despite compromising over 1,000 entities and earning nearly $300 million in ransoms, the group faced significant setbacks due to FBI infiltration. The FBI gained access to critical encryption keys through a confidential informant. Resultingly, LockBitSupp, manager of LockBit, is trying to recruit their affiliates.	Following on from the Q1 disruption of Hive, we see the disruption of BlackCat, our most impactful group of 2023. In 2023, authorities intensified their efforts against the groups. Some think their actions have limited impact, with few arrests and ongoing rumours of their continued activity. However, it disorganises the groups and creates distrust and insecurity among the members and affiliates. Resultantly, they will lose affiliates and members to other groups.

*Note that claims incidents in the news are not necessarily Hiscox claims, but are examples sourced from publicly available information.

Top Hiscox claims trends

Financial fraud and data breach were the top claim impacts in 2022 and in 2023. Although both had less dominance in claims in 2023. Financial fraud and data breaches made up 57% of claims in 2022, this decreased to 48% in 2023.

1 Extortion

Extortion remained the primary cost factor in both the current and preceding years, with 70% of losses in 2022 attributed to extortion, slightly decreasing to 69% in 2023. The USA bore the highest expenses, accounting for 52% of extortion losses, followed by the UK at 26% and Europe at 22%. The most prominent ransomware variants encountered by our insured were Lockbit, Blackcat, and ESXiArgs. Compared to 2022, the count of ransomware incidents remained at the same level. Similarly, there was no change in the number of ransomware claims in Europe. However, the UK saw a 22% surge, while the USA experienced an 18% decrease.

Real-life scenario

Our insured experienced a Lockbit 3.0 ransomware incident. The insured rapidly moved to recovery, which resulted in a relatively minimal business impact. The insured had correctly segmented and secured their backups, meaning they were still viable after the incident. Half a day of data had been lost. Losses were incurred through forensics, to determine the initial entry point and review what data was stolen. As a result of the hackers' actions and the insured actions, log evidence was lost so a concrete root cause could not be defined. However, our forensics partner identified the various possible causes and helped mitigate them to help prevent future attacks.

2 Financial fraud

Financial fraud was the most common type of claim, accounting for 27% of all claims made by our insureds. Nevertheless, it only makes up 12% of claims costs. Compared to 2022, there was an overall 25% decrease in the number of claims. Although the average claim was more costly, with a 4% increase. Spear phishing was the leading cause of financial fraud, equalling 48% of these losses, followed by entry using non-phishing social engineering and compromised credentials, which incurred 22% and 18% respectively of financial fraud losses.

Real-life scenario

An email account of a supplier to our insured was compromised. The threat actor (TA) was monitoring communications on the supplier's account waiting for an exchange of invoices. Eventually the supplier sent over a legitimate invoice for their services to our insured. The TA then shortly followed with a request for the insured to send the funds to a different bank account. The insureds finance team complied with the change request, sending the funds to the illegitimate TA's account.

3 Data breach

2023 data breach claims were relatively low with claims count and losses decreasing year on year by 36% and 52% respectively. In 2023, these claims were 20% of all claims and 7% of all losses. Breaches caused by insiders were 24% of losses, supply chain was the most common and was also 24% of losses. Europe (63% of data breach claims) was most frequently affected by data breaches, followed by the USA (19%) and the UK (18%).

Real-life scenario

Our insured became aware that within their website a threat actor had created another few boxes at checkout for bank account details before the customer is redirected to enter bank account details securely, as per normal procedures. The insureds third-party IT suppliers investigated this matter discovering over 50 customers had placed an ordered since. This resulted in the bank details of a client of our insured leaking, who subsequently needed to be notified.

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. In 2023, supply chain attacks were the fifth most common point of entry for a claim, followed by system vulnerabilities. Companies should pause and take the time to audit their vendors and patch/update the services they use. It's important that companies apply all recommended updates and patches, also imploring their vendors to do the same, to decrease risk and defend against attacks once a known vulnerability has been exploited.

Promote a culture of cyber awareness

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 mitigated when staff are aware of security risks and the techniques used to exploit employees. People are the heart of the business, fostering cyber resilience will ensure that the people in the business can resist attacks. 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 BEC 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.

Understand your exposure

Previously, remote desktop protocol (RDP) was a key driver in ransomware attacks and subsequent data exfiltration. However, we are now seeing an increase in incidents where the point of entry is through systems exposed to the internet. This can occur due to vulnerabilities or simply because systems that should not be exposed are accessible.Generally, we observe fewer incidents when organisations audit and manage the services exposed on their network perimeter. Understanding your assets allows you to better inform your patching policy. Additionally, leveraging threat intelligence can enhance security posture by providing insights into emerging threats and the tactics, techniques and procedures used by threat actors.

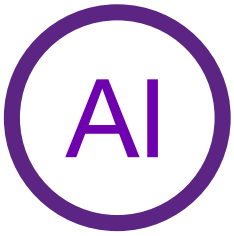
Big business update

For larger companies with customers over 20,000 employees, claims volumes for cyber incidents were lower than anticipated in 2022 and remained less volatile in 2023. The conflict between Russia and Ukraine appeared to have disrupted several threat groups earlier in 2022, and although some of these groups have re-formed or established alternative groups in 2023, there was no significant uplift in attacks. IT forensic and incident response specialist lawyers have reported an increase in activity in the second half of 2023, however, and we remain vigilant for increases in incident notifications.

BIPA, Meta Pixel and wrongful data collection claims continue to grow, with non-breach regulatory violation coverage becoming more of a concern. Plaintiff firms are using various legislation, often 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 US. We continue to expect data protection claims to continue to rise in volume and severity as we go into 2024. As noted previously, coverage for fines will depend on wordings and applicable jurisdictions.

Increase in exfiltration ransomware

Instead of encrypting victims' files, some threat actors are opting to threaten data leaks and demand payments in exchange for not disclosing stolen information. In the Hiscox Cyber Readiness Report 2023, for large businesses over 250 employees, 46% paid a ransom to protect customer data, while 42% of smaller businesses with less than 250 employees say it was to protect confidential company data. Fewer companies paid to be operational again.

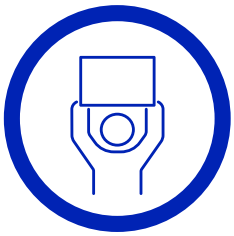


The positives and negatives of artificial intelligence (AI)

Large language models (LLMs) accelerate the learning curve for malicious actors, aiding in the creation of sophisticated custom malware, utilisation of hacking tools, and in composing coherent and convincing phishing emails. Dedicated tools tailored for black hat activities, such as WormGTP, underscore their impact. However, it's not all doom and gloom. While AI can empower hackers, it can also play a crucial role in developing and deploying innovative security software and reinforcing existing defences against evolving threats. AI contributes to automating threat detection in email systems and networks, analysing user activities and behaviour for signs of malicious intent.

Payment diversion fraud (PDF) continues to be a challenge

According to our own report data, one-in-three companies attacked experienced PDF, which has now taken the top spot for outcomes of a cyber attack. PDF involves manipulation or deception tactics to induce employees into redirecting legitimate payments to fraudulent accounts. It was the second most common outcome in the previous two years. Defending against social engineering attacks like email phishing and SMS phishing (so-called smishing) through employee training is a key way to manage this risk.



Managing political activists

The International Committee of the Red Cross (ICRC) released the first-ever set of rules of engagement for civilian hackers involved in conflicts, warning against a surge in patriotic cyber attacks, particularly in the wake of the Ukraine invasion and now the Israel-Hamas conflict. Threat actor groups with ideological motivations have, and will disrupt, various sectors including banks, businesses, hospitals, railways, and government services of ideological opponents and their allies. The threat these actors pose is a legitimate risk, with various groups on both sides of conflicts engaging in cyber attacks there is potential for this to spill into uninvolved organisations. While certainly not all hacktivists will adhere to these rules, they establish an ethical and legal framework, providing a basis for condemning unacceptable actions, promoting responsible hacktivism, and preserving essential ethical standards in the hacktivist community.

Advanced malware avoids detection

Since the mainstream adoption of behaviour-based endpoint detection and response (EDR) technologies, we have observed a decline in the effectiveness of traditional malicious software (i.e. malware, viruses). Nevertheless, a shift is emerging, wherein malware adopts tactics that do not generate the alerts such as using commercial software for malicious purposes (e.g. remote access and file transfer software. This evolution in malware behaviour is anticipated to continue, giving rise to more sophisticated and elusive forms of malware.

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

22803 07/24