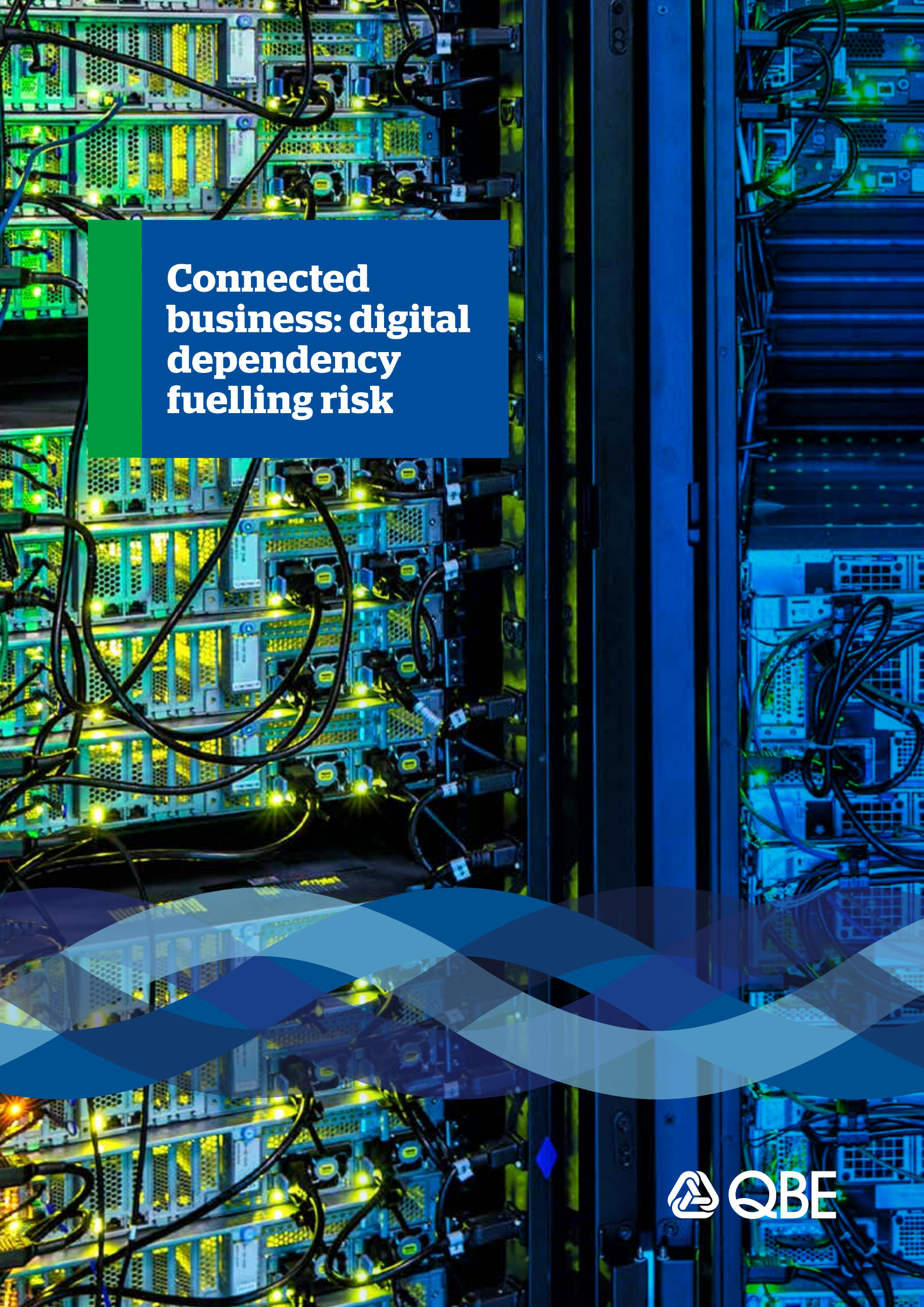


Connected business: digital dependency fuelling risk

QBE

Introduction

People and organisations around the world increasingly rely on digital technologies. Computers and artificial intelligence (AI) tools are enabling and automating both simple and complex business tasks as smart devices connect factories, vehicles and other equipment to the internet.

Global technology markets will grow exponentially in the coming five years. The AI-as-a-service market is set to grow ninefold from approximately USD 200bn to 1.85tn, software-as-a-service threefold to USD 850bn and infrastructure-as-a-service fivefold to USD 532bn, demonstrating the scale of opportunity presented by emerging digital technologies.

However, cybercriminals have been stealing sensitive data to extort and defraud businesses of all sizes and in all sectors, while other malicious actors have been using technology to disrupt their opponents and push their ideological narratives.

Global technology disruption

The mass outage affecting systems running CrowdStrike's Falcon Sensor on 19 July has brought the interdependence and vulnerability of global technology systems starkly into focus. The outage has cost Fortune 500 companies an estimated USD 5.4bn worth of damage and USD 25bn in share value – not including Microsoft.

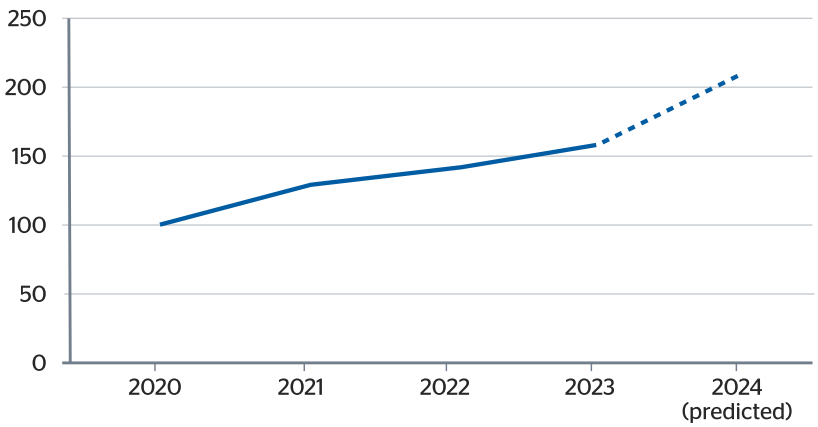
CrowdStrike's faulty content update knocked out around 8.5m Windows computers, less than 1% of all Windows devices, disrupting industries worldwide but most severely aviation, transport and healthcare. Cybercriminals jumped on the opportunity to launch phishing campaigns with CrowdStrike-related lures, seeking to compromise systems, steal data and extort victims. In this instance, the CrowdStrike incident was an error rather than an intentional disruption – but many cyber incidents are and will be intentionally disruptive.

In June 2017, the NotPetya mass cyber attack targeted Ukrainian organisations but ultimately resulted in infections across Europe, North America and Asia Pacific. The NotPetya malware, which masqueraded as ransomware, affected critical sectors such as transport, logistics and shipping, causing an estimated USD 10bn in damages. While it hit far fewer devices than the CrowdStrike incident, its intentional nature led to a higher degree of disruption.

As technology interdependencies grow, we expect more cyber incidents to disrupt many companies in a single attack, meaning businesses are more likely to experience a disruptive cyber event. Malicious actors can also target specific companies to cause greater damage, whether they're extorting ransoms or destabilising geopolitical rivals.

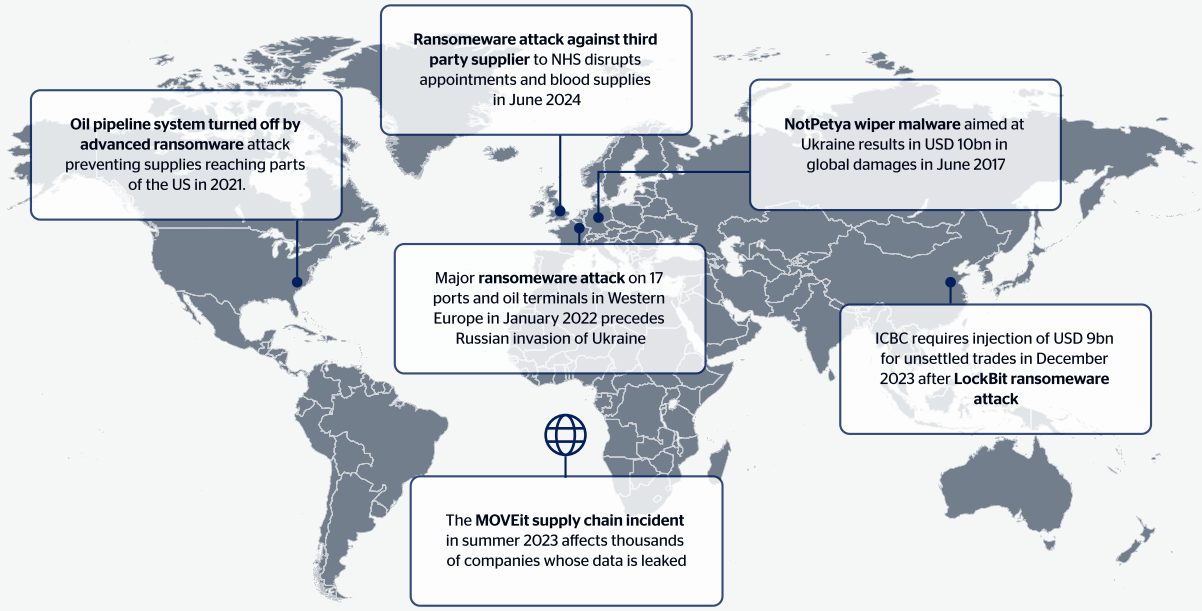
> The CrowdStrike outage has cost Fortune 500 companies an estimated USD 5.4bn worth of damage and USD 25bn in share value

Number of recorded destructive and disruptive cyber attacks, since 2020



Source: Control Risks

Significant disruptive cyber threat incidents, since 2017



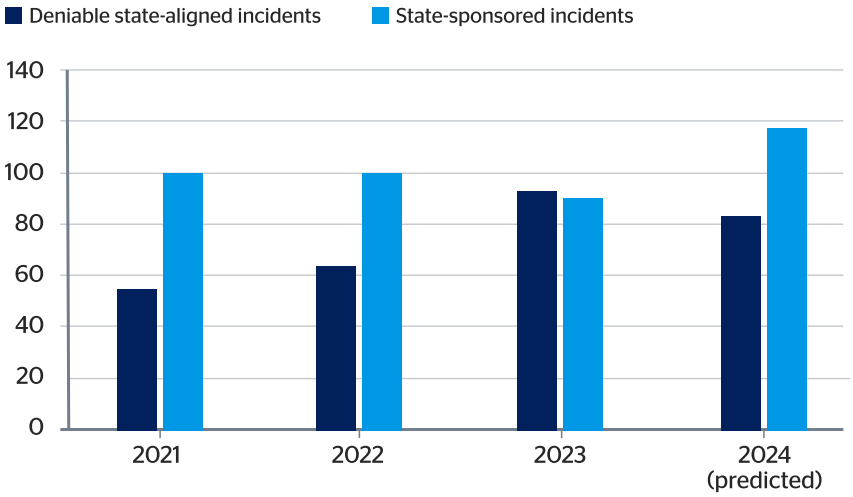
Spillover attacks

Greater geopolitical competition is making the world increasingly multipolar. State-linked cyber actors have growing intent to disrupt critical national infrastructure (CNI), for example through ransomware. Such attacks can be driven by geopolitical events like the ongoing Israel-Hamas or Ukraine-Russia conflicts, manifesting as state-directed cybercriminal or activist attacks against entities in strategic sectors outside the theatre of conflict. Energy sector organisations are highly attractive targets for spillover cyber attacks, which can destabilise financial markets and governments.

Energy sector organisations are highly attractive targets for spillover cyber attacks, which can destabilise financial markets and governments

Some states have assigned resources to maintain cyber activist personas for disruptive and destructive attacks, in an effort to maintain plausible deniability, as they seek to shield themselves from attribution or diplomatic penalties. CNI organisations are attractive targets for spillover threats as threat actors feel they can disrupt them without necessarily provoking a battlefield response. Espionage units masquerading as financially motivated ransomware groups are also proliferating, reinforcing the high state-linked threat to sensitive intellectual property and corporate data.

Number of significant non-state proxy attacks and recorded state-linked campaigns, since 2021



Source: Control Risks

Russia-linked ransomware attacks on 17 European oil terminals ahead of Ukraine invasion

A series of large-scale ransomware attacks targeted port terminals in Belgium, Germany and the Netherlands in January 2022. Highly likely to have originated from Russia-sponsored actors, the attacks knocked out IT systems, affecting the ports' operations in loading oil products. The attacks were carried out three weeks before Russia's invasion of Ukraine, illustrating how spillover attacks target secondary sectors and geographies.

Ransomware attacks in 2023 were up 74% on 2022

Drivers of growing cyber threat incidents

Geopolitics

US-China tensions, growing multipolarity and ongoing conflicts drive disruptive spillover globally against intentional and inadvertent victims

Ransomware

Cybercrime gangs are more active and disruptive than ever with a high volume of attacks, huge revenues and greater ransom demands

Third-party threats

Infrastructure providers, software serviced, data hosts and technologies are the cyber frontline and increasingly the priority targets

Technology

AI advancements quickly introduce new risks, while increasing connectivity and interdependence grows the ever-expanding attack surface.

Control Risks

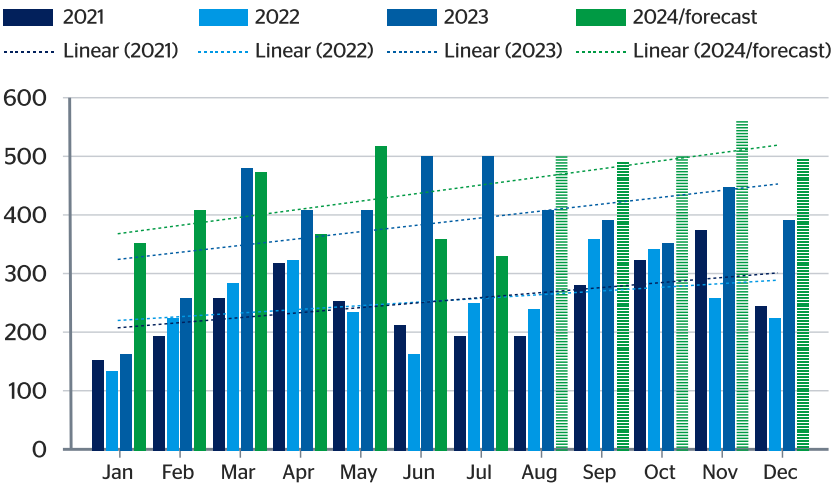
Ransomware

Revenue up as number of attacks increase

Ransomware attacks in 2023 were up 74% on 2022, and total ransom payments made by victims exceeded USD 1bn globally. After law enforcement took down the Hive group in 2022, the cybercriminal ecosystem fragmented and ransomware code was leaked, enabling lower-capability groups to conduct their own attacks.

This ransomware resurgence has continued in 2024, with the number of publicly named victims reaching the highest monthly totals in the last three years *(*note the graphic below includes MOVEit, a 2023 incident that led to a high volume of victims. In real terms, 2024's numbers are significantly higher than 2023 if the MOVEit incident is disregarded as an anomaly.)*

Number of ransomware victims named on data leak sites



Source: Control Risks

Number of publicly named victims by ransomware and data leak extortion groups

2021	2022	2023	2024 (forecast)	2025 (forecast)
2,964	2,981	4,698	4,800	5,200

Source: Control Risks

Sectoral analysis

Ransomware attacks heavily targeted the manufacturing, healthcare, IT, education and government sectors in 2023. As resilience varies between sectors, attackers are increasingly targeting across sector verticals but focusing on manufacturing and healthcare, where operational disruption has punishing impacts.

Ransomware poses a high threat to manufacturing and production organisations, with 65% of the sector having reported a ransomware attack in 2023, with an average ransom payment of USD 2.4m. Among victims in the sector, 62% paid ransoms to retrieve stolen data.

> Healthcare organisations facing ransomware attacks increased from 214 in 2022 to 389 in 2023, an increase of 81.7%

There is insufficient intelligence to accurately calculate the average demand as this will vary significantly between geographies, sectors and organisations. However, large organisations that are highly vulnerable to operational disruption will highly likely face ransom demands in the tens of millions of USD, and smaller organisations in the hundreds of thousands. Organisations facing the highest ransom demands are likely to be in the healthcare, government, IT and communications and manufacturing sectors.

Healthcare organisations are also highly attractive, as are those holding large volumes of personally identifiable information (PII) and protected health information (PHI) and those with critical uptime requirements. Such targeting is also driven by the perception that the healthcare sector has comparatively weaker cyber security maturity than other industries. The number of healthcare organisations that faced a ransomware attack increased from 214 in 2022 to 389 in 2023, an increase of 81.7%.

Big game hunting

Ransomware groups are increasingly using “big game hunting” tactics, identifying high-revenue and high-profile entities to extort in their attacks. Big game hunting allows ransomware groups to increase their average ransom payment through higher initial demands than a small and medium-sized enterprise could afford, as well as leveraging operational disruption to large numbers of these victims’ clients and/or customers.

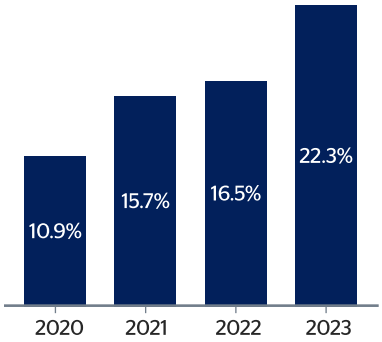
In recent years law enforcement has achieved greater success in disrupting ransomware groups, as exemplified by the takedown of the Hive ransomware and partial takedowns of the prolific LockBit and BlackCat groups. Ransomware groups have therefore sought to maximise ransom payments through big game hunting before law enforcement agencies catch up with them and seize their assets and infrastructure. The average ransom payment in 2023 increased to USD 2m compared with USD 400,000 the previous year. The average has been significantly impacted by big game hunting, as some threat actors have demanded upwards of USD 50m. However, the median ransom demand has remained the same, at around USD 300,000.

Threat actors also see large organisations as more likely to pay a ransom. On average, 61% of organisations with an annual revenue of USD 5bn pay out ransoms after an attack, compared with 25% of organisations with an annual revenue totalling less than USD 10m. Some high-revenue victims perceive operational disruption as more costly than paying a ransom.

LockBit attack on ICBC illustrates opportunistic ransomware threat to finance sector

The LockBit ransomware group targeted the US-based financial services arm of the Industrial and Commercial Bank of China (ICBC) in November 2023, disrupting trading in the US Treasuries market. This included the forced re-routing of financial trades and prevented ICBC Financial Services from settling Treasury trades for other market traders, meaning ICBC had to inject USD 9bn to its US unit. Attackers likely infiltrated ICBC's network via an unpatched Citrix NetScaler box that enabled them to bypass authentication measures.

Proportion of global cyber incidents impacting third-party IT providers (2020-23)



Source: Control Risks

Supply chain compromise

Third-party incidents

At least 22% of all cyber security breaches in 2023 were likely the result of follow-up targeting from third-party incidents. To manage this third-party risk, which is difficult to mitigate, organisations must adopt best practices internally to strengthen their resilience from external breaches and follow-up targeting after major incidents, while also considering the risk posture, mitigation strategies and insurance policies of their third-party IT providers.

Sector

For cybercriminals and state-linked threat actors, IT providers, such as software-as-a-service (SaaS) organisations, are a prime target. In 2023, 75% of third-party incidents originated from attacks on service and software providers.

Share of reported third-party breached in 2023, by sector

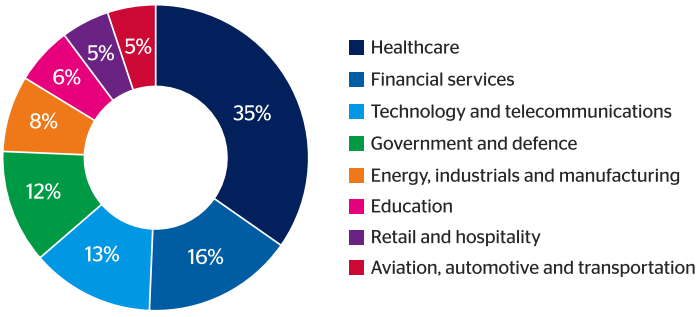


Chart: Control Risks • Source: Security Scorecard

Over 75% of third-party incidents in 2023 are attributable to just three supply chain vulnerabilities

Zero-day attacks can be most impactful for ransomware groups

Ransomware groups see IT supply chains as attractive targets due to the opportunity to hit many organisations across sectors through a single attack. Such organisations have high uptime requirements, which can be leveraged in ransom negotiations. In 2023, 64% of third-party breaches were linked to the Clop ransomware group exploiting a zero-day bug (an unknown and unpatched vulnerability in a system or device), and 61% of third-party breaches were attributed to the MOVEit vulnerability, highlighting how third-party risks can evolve into direct impacts on supply chain customers. The chart below shows that more than 75% of third-party incidents in 2023 are attributable to just three supply chain vulnerabilities.

Share of reported third-party incidents in 2023, by vulnerability

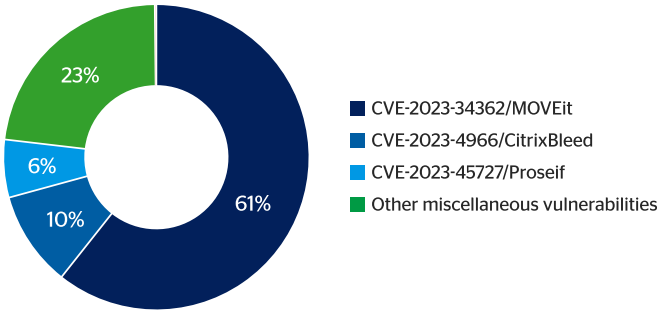
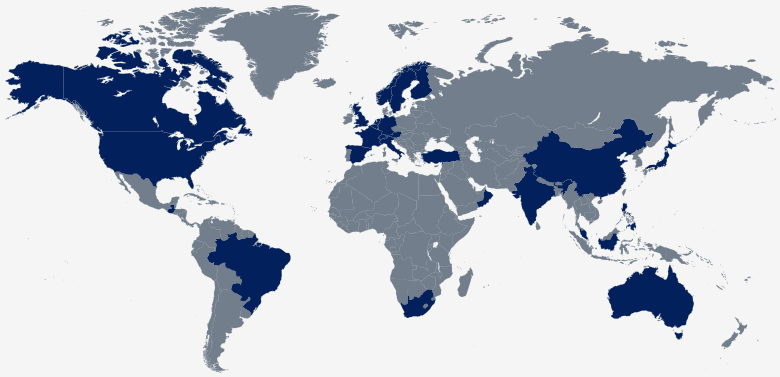


Chart: Control Risks • Source: Security Scorecard

MOVEit campaign shows breaching IT providers' data can have wide-ranging impact

After exploiting a zero-day vulnerability in the MOVEit file transfer service in May 2023, the Clop cybercriminal group stole files from organisations unaware they were exposed to that vulnerability. The wave of data theft and data leak extortion incidents affected at least 2,180 organisations. Clop likely collected over USD 100m in ransom payments.

Geographic spread of MOVEit victims



Technology

Cloud threats

Since organisations have adopted cloud services, threat actors have developed tools and tactics to gain easier and more persistent access to cloud-based applications, to explore an infected network and find further vulnerabilities. Navigating through cloud-based setups also allows them to evade typical detection protocols such as advanced IP analysis. State-linked actors and sophisticated cybercriminals have also moved to the cloud themselves, exfiltrating data to their own cloud storage.

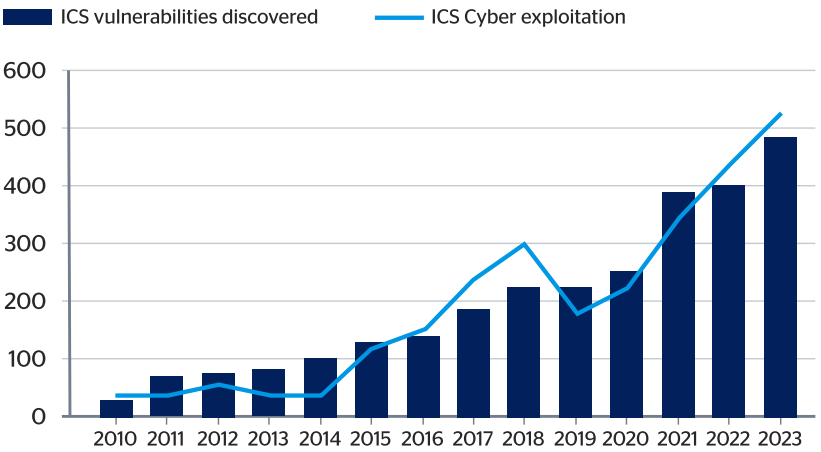
Operational technology and IoT adoption

Ransomware attacks against industrial sector organisations increased by 50% in 2023 compared with 2022. Successful attacks that disrupt operational technology (OT) – the software and hardware that monitors and controls industrial equipment – help cybercriminals extort payments, as the operational disruption is more financially punishing than the ransom. OT disruption can also fulfil strategic objectives for state-linked actors. Disrupting manufacturing processes can prove to be lucrative or strategically valuable – or both.

Engineering, manufacturing and utilities are all attractive targets for attacks affecting OT. Threat actors of varying capabilities have increasingly targeted OT that uses internet-exposed controllers or devices. A marked proliferation in internet-of-things (IoT) devices – hardware connected wirelessly to networks – likely exacerbated such threats to OT, particularly in the manufacturing and utilities sectors. Effective network segmentation and a limit on or complete removal of internet-exposed ports reduces the risk of a disruptive attack on OT.

Ransomware attacks against industrial sector organisations increased by 50% in 2023

Number of vulnerabilities in ICS vs incidents exploiting ICS vulnerabilities, 2010-23



Source: Control Risks

> Organisations will increasingly leverage generative AI and automation techniques to identify cyber attacks

AI

From solely pre-programmed AI tools for specific tasks that require human input, AI is currently developing into limited memory or narrow AI, which can use mass datasets to make decisions. For instance, open-source generative AI tools can write code for malware or enhance many of the traditional tactics employed by state-linked threat actors and cybercriminal groups, such as spearphishing and malware attacks.

As AI becomes more readily accessible and large language models (LLMs) proliferate, lower-capability threat actors like cybercriminals and cyber activists will be able to launch larger attacks more quickly. This capability uplift in scale and pace will be the most significant impact on the cyber threat landscape.

Criminals are deploying generative AI tools to create deepfakes of trusted employees and executives to defraud organisations of all sizes. Earlier this year a global organisation lost USD 20m through a deepfake attack. These schemes aren't new, with some reported as early as 2019, but their frequency and chances of success are growing substantially; the skills required to carry them out decrease as the technology improves.

Conversely, AI already plays a part in detecting malicious behaviours in corporate networks, and we expect it will continue to improve cyber security capabilities generally with increased efficiency of security and defensive activities. Organisations will increasingly leverage generative AI and automation techniques to identify cyber attacks against an innovative, motivated and ever-changing threat landscape.

Diversification of technologies

Cloud and emerging technologies have provided organisations with cost-effective infrastructure solutions. However, the wider adoption of infrastructure-as-a-service and AI-as-a-service has added to threat actors' attack surface, offering greater opportunity to infect multiple victims per incident.

A rise in IoT devices has enabled more disruptive cyber attacks to impact essential public services, such as water distribution. Advances in generative AI have enabled cybercriminals to create deepfakes of executives to facilitate social engineering attacks. State-linked threat actors and cyber activists are turning to cybercriminal solutions to influence elections or fund campaigns. A wider array of threat actors are developing their own tools and leveraging AI to automate attack preparation and deploy malware. The adoption of emerging technologies at varying degrees of pace and scale depending on sector and geography is widening an attack surface, while organisations scramble to maintain readiness.

Activists target operational technology and cut off water supply

In December 2023, the Iran-linked activist group Cyber Av3ngers targeted a private water scheme in Erris, Ireland. Exploiting programmable logic controllers (PLCs) manufactured by Israeli company Unitronics, the attacks resulted in a two-day outage of water to local residents. Cyber Av3ngers claimed the attacks affecting PLCs as part of their campaign targeting Israeli products and organisations amid the Israel-Hamas conflict.

Conclusion

Technology interdependence, driven by advances in interconnectivity, AI and emerging technologies, has provided opportunities for cyber actors to impact businesses. A digital transformation strategy secured against future threats can be the catalyst for success. Unstable global conflicts, geopolitical shifts and a booming cybercriminal economy are all likely to propel greater risks to organisations adopting emerging technologies into working practices.

Interdependency across sectors and businesses will make such risks unavoidable, as threat actors prioritise developing sophisticated malware to impact OT environments or third-party providers of services and software. AI and other technologies will continue to develop, helping to reduce and prevent a range of threats seeking to leverage technology interdependence. Risk mitigation strategies must consider the increasing likelihood of cyber incidents, and proactively push for resilience while implementing response protocols to react swiftly to cyber incursions.

Annex – key references

"Global ransomware threat expected to rise with AI, NCSC warns", ncsc.gov.uk
"2023 Ransomware Attack Report", blackfog.com
"Ransomware Payments Exceed $1 Billion in 2023, Hitting Record High After 2022 Decline", chanalysis.comv
"#StopRansomware: CLOP Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability", cisa.gov
"Two-day water outage in remote Irish region caused by pro-Iran hackers", therecord.media
"NCC Group Releases Annual Cyber Threat Monitor Report 2023", nccgroup.com
"Ransomware Attacks Surge in 2023; Attacks on Healthcare Sector Nearly Double", dni.gov
"The State of Ransomware 2024", sophos.com
"The State of Ransomware in Manufacturing and Production 2024", sophos.com
"Helping our customers through the CrowdStrike outage", blog.microsoft.com
"Dragos 2023 OT Cybersecurity Year in Review", dragos.com
"Global Third-Party Cybersecurity Breach Report", securityscorecard.com

A correction was published on 9 October 2024 to rectify an erroneous figure in the sectoral analysis on p. 7. Globally, a total of 389 healthcare organisations faced ransomware attacks in 2023 (Control Risks, 2024)

QBE Cyber Insurance

QBE's cyber products protect against the range of risks associated with digital technology and provide critical support in the event of a cyber-attack. The offering includes QCyberProtect, a new global cyber insurance policy for consistent coverage worldwide, for losses arising from current and emerging cyber risks, including, but not limited to, network security, privacy liability, IT and non-IT business interruptions and reputational loss.

Tailored cover and individual service

To ensure you are protected, QBE's underwriters work closely with customers to create cover that suits specific needs. We take the time to understand your business to provide bespoke cover that protects you against current and emerging cyber risks.

Helping you manage your risks

We don't just cover risks; we help you to manage and reduce them. We offer risk management support tools including:

- QBE QCyberPrepare – an online saferoom to help customers prepare for a cyber incident.
- Free access to the QBE Cyber Risk Management Portal, which offers a wide range of information on cyber risks as well as how to make sure you're protected against them.
- Access to QBE tools and services, as well as discounts for a range of Cyber Risk Management Services from our trusted partners.

Crisis support

QBE provides 24-hour support if you experience a cyber event. That might involve providing a forensics team to work out how the cyber breach happened and how to fix the problem; legal advice to address regulatory requirements; or managing a media statement to minimise any impact to your reputation.

For more information, visit **QBEeurope.com**

This report has been developed for QBE by **Control Risks**

QBE European Operations
30 Fenchurch Street
London EC3M 3BD
+44 (0)20 7105 4000
QBEeurope.com

641209/2405