Sponsored by

QBE

CIR
CONTINUITY INSURANCE & RISK

Digital dependency fuels risk
David Warr examines the likely implications of emerging cyber and AI threats for businesses, and explores how cyber security must evolve alongside a growing reliance on digital technologies

Seven ways businesses can manage AI risks
Jaini Gudhka outlines a number of practical measures that businesses could – and should – be implementing now to mitigate the emerging risks of using generative artificial intelligence

Cyber and AI risks

QBE

Sponsored by

Digital dependency fuels risk

David Warr examines the likely implications of emerging cyber and AI threats for businesses, and explores how cyber security must evolve alongside a growing reliance on digital technologies

Global technology markets will grow exponentially in the coming five years, as people and organisations around the world increasingly rely on digital technologies. The AI-as-a-service market is set to grow ninefold from approximately US$200 billion to 1.85 trillion, software-as-a-service threefold to US$850 billion and infrastructure-as-a-service fivefold to US$532 billion, demonstrating the scale of opportunity presented by emerging digital technologies.

At the same time, cyber criminals have been stealing sensitive data to extort and defraud businesses everywhere, while other malicious actors have been using technology to disrupt commercial organisations and national infrastructures.

Global disruption

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

CrowdStrike's faulty content update knocked out around 8.5 million Windows computers, less than one per cent of all Windows devices, disrupting industries worldwide, and the aviation, transport and healthcare industries especially. Cyber criminals 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 malicious – but many cyber incidents are, and will continue to be, intentionally disruptive.

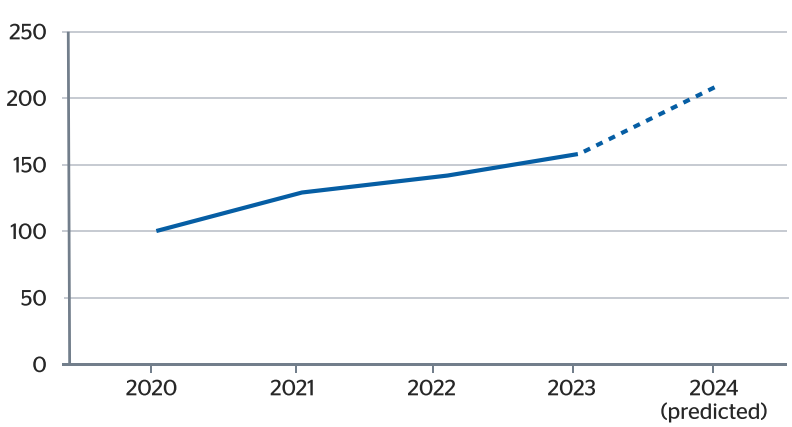
In June 2017, the NotPetya mass cyber attack targeted Ukrainian organisations but ultimately resulted in infections across Europe, North America and Asia Pacific, affecting critical sectors such as transport, logistics and shipping. It caused an estimated US$10 billion in damages. While it hit far fewer devices than the CrowdStrike incident, its intentional nature led to a higher degree of disruption.

State-linked cyber actors have growing intent to disrupt critical national infrastructure, including through ransomware. Such attacks can be driven by geopolitical events, such as the ongoing Israel-Hamas and Ukraine-Russia conflicts, manifesting as state-directed cyber criminal or activist attacks against entities in strategic sectors outside the theatre of conflict.

CNI organisations are often targeted as threat actors feel they can disrupt them without necessarily provoking a battlefield response, with the energy sector particularly attractive to cyber attackers, as a means of destabilising markets and governments.

Ransomware resurgence

Ransomware attacks in 2023 were up 74 per cent year-on-year, with total ransom payments made by victims exceeding US$1 billion globally. After law enforcement took down the Hive group in 2022, the cyber criminal 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.



Source: Control Risks

Sectoral analysis

Ransomware attacks heavily targeted the IT, education, government, manufacturing and healthcare sectors in 2023, with the latter causing particularly punishing operational disruption.

Ransomware poses a high threat to manufacturing firms, with 65 per cent of the sector having reported a ransomware attack in 2023, with an average ransom payment of US$2.4 million. Some 62 per cent paid ransoms to retrieve stolen data.

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, and smaller organisations in the hundreds of thousands.

Healthcare organisations are highly attractive targets, as are others holding large volumes of personally identifiable information and protected health information, and those with critical uptime requirements. Such targeting is also driven by the perception that the healthcare sector has comparatively less mature cyber security than other industries. The number of healthcare organisations that faced a ransomware attack was up over 81 per cent from 214 in 2022 to 389 in 2023.

Big game hunting

Ransomware groups are increasingly using 'big game hunting' tactics in their attacks, identifying high-revenue and high-profile entities to extort their victims. Big game hunting allows ransomware groups to increase their average ransom payment through higher initial demands than an SME might afford, as well as leveraging operational disruption to large numbers of victims' customers.

In recent years, law enforcement has achieved greater success in disrupting ransomware groups. These groups have therefore sought to maximise ransom payments through big game hunting before law enforcement agencies catch up with them. The average ransom payment in 2023 increased to US$2 million from US$400,000 the previous year. The average has been significantly impacted by big game hunting, as some threat actors have demanded upwards of US$50 million. The median ransom demand has remained the same, at around US$300,000.

On average, 61 per cent of organisations with an annual revenue of US$5 billion pay out ransoms after an attack, compared with 25 per cent of organisations with an annual revenue totalling less than US$10 million, perceiving the operational disruption to be more costly.

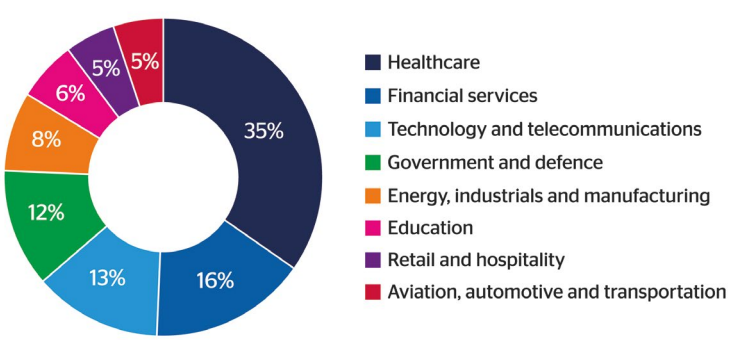
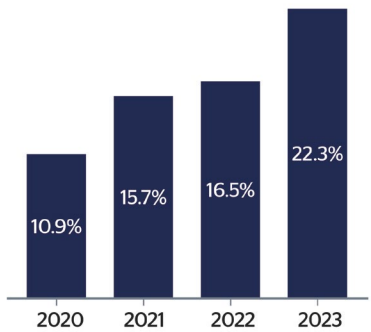


Chart: Control Risks • Source: Security Scorecard



Source: Control Risks

Supply chain incidents

At least 22 per cent 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, 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.

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

Cloud threats

The cloud services boom has led threat actors to develop 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 cyber criminals have meanwhile also moved to the cloud themselves, exfiltrating data to their own cloud storage.

OT and IoT adoption

Ransomware attacks against industrial sector organisations increased by 50 per cent in 2023 compared with 2022. Successful attacks that disrupt operational technology – the software and hardware that monitors and controls industrial equipment – help cyber criminals extort payments, as the operational disruption is more punishing than the ransom.

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 IoT devices 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.

Artificial intelligence

AI uses 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 cyber criminal groups, such as spear-phishing and malware attacks.

As AI becomes more accessible and large language models proliferate, lower-capability threat actors like cyber criminals and cyber activists may 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 US$20 million through a deepfake attack. These schemes aren't new, 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. Further, organisations will increasingly leverage GenAI and automation techniques to identify attacks against an innovative, motivated and evolving threat landscape.

Diversification of technologies

The adoption of infrastructure-as-a-service and AI-as-a-service has offered cyber attackers a greater opportunity to infect multiple victims per incident.

A rise in IoT devices has enabled more disruptive attacks to impact essential public services, such as water distribution. Advances in generative AI have enabled cyber criminals to create deepfakes to facilitate social engineering attacks. State-linked threat actors and cyber activists are turning to criminal solutions to influence elections or fund campaigns. Threat actors are developing their own tools and leveraging AI to automate attack preparation and deploy malware. The adoption of emerging technologies is widening the attack surface, while organisations scramble to maintain readiness.

Advances in interconnectivity, AI and emerging technologies have 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 cyber criminal 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.

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 an attack. The offering includes QCyberProtect, a new global cyber insurance policy for consistent coverage worldwide, for losses arising from current and emerging cyber risks.

QBE offers support tools including:

- QBE QCyberPrepare – an online saferoom to help customers prepare for a cyber incident
- Tailored tabletop incident response planning sessions, focussing on individual client exposures and challenges – hosted by QBE's dedicated in-house Cyber Services team
- QBE 24-hour crisis support

For more information, visit: https://qbeeurope.com/products/cyber/

David Warr, portfolio manager, QBE Europe

Seven ways businesses can manage AI risks

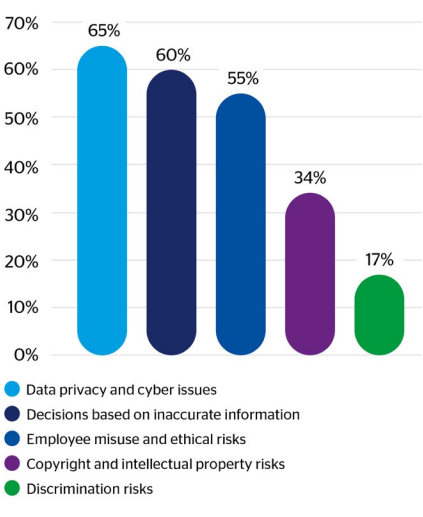
Jaini Gudhka outlines a number of practical measures that businesses could – and should – be implementing now to mitigate the emerging risks of using generative artificial intelligence

For businesses, generative artificial intelligence is both exciting and daunting. Users of GenAI are expected to reach 77.8 million in the two years following the November 2022 release of ChatGPT – which is more than double the rate of uptake for mobile phones at the height of their user adoption.

Undoubtedly, GenAI can offer a competitive edge, by speeding up operations for instance. But this fast-evolving technology poses new risks to data privacy, intellectual property or sound decision making. While businesses are increasingly looking to engage with the new opportunities that AI offers, many are simultaneously grappling to understand and manage the full risk landscape that it operates within.

Research conducted in 2023 by Riskonnect revealed that although 93 per cent of surveyed companies were aware of AI-related dangers, only 17 per cent had briefed their workforce or implemented any training – and only nine per cent believed that their organisation was prepared for these risks.

While uncertainty around AI might lead to some to try a 'wait and see' approach, risk managers should be thinking carefully now about how GenAI applications are being applied to internal and external business operations in more detail. Short- and long-term planning should combine a robust risk management framework alongside structured scenario testing to address potential dangers.



Source: Riskonnect's 2023 New Generation of Risk Survey

To support entrepreneurs and risk professionals looking to experiment with GenAI in a safe way, we have compiled a seven-point check list to mitigate the risks:

1) Choose your tool

Many AI tools will capture the data input for their own machine-learning processes. Make sure the one you select meets client confidentiality and information security standards. The National Cyber Security Centre provides some guidelines for secure AI system development.

Include data and cyber requirements in your Service Level Agreement and consider contractual protections if your own service delivery model will rely on output from an AI tool.

2) Do your due diligence

When selecting the third-party providers that will have access to your and your clients' data, check their AI safeguards.

3) Detail your data

Keep a record of what data you have, its quality, value and where it is stored.

Consider checking:

- Is your data relevant and adequate for your needs? Is it reliable?
- Do you need additional sources and, if so, which sources?
- Is the data held in silos?
- Has it been corrupted or infiltrated?

You should include a detailed data strategy in your AI risk management plan, and use a diversity of sources to mitigate the risks of bias.

4) Polish your policies

Keep accountability and governance front and centre when updating policies and procedures.

Update your acceptable use documentation to specify which AI tools can be used, on what devices, and for what purposes.

Review supervision processes and ensure that AI-assisted outputs are checked by a person on a risk-assessed basis.

Test your data security regularly, using trusted independent agencies to assess vulnerabilities. Include misuse of AI in your disciplinary processes.

Last but not least, include AI in your risk register.

5) Beat breaches

Use multi-factor authentication and digital certificates to secure communications

Set up internal-only channels for colleagues to share documents

For important actions, such as high-value bank transfers, have a process requiring the operation to be verified via a secure communication channel, that is not initiated by the requester.

6) Educate your employees

Regular training is essential for employees to help defeat breaches. People must be familiar with the AI tools that the business has approved for use, and the associated workflows, processes and risk controls. They should also be aware of the wider implications. When used inappropriately, AI might lead to error replication and bias reinforcement. So critical assessment skills are crucial to identify errors, hallucinations or bias. That should be on top of AI literacy and data management training

Employees should also be wary of such innovations as deepfakes and the various ways in which criminals can also use AI, as these can have a considerable impact on cyber security.

"Regular training is essential to defeating breaches. People must be familiar with the AI tools that the business has approved for use, and the associated workflows, processes and risk controls"

7) Take cover

Purchasing a cyber insurance policy not only helps businesses transfer emerging risks; it also gives them access to a range of associated services and expert advice to better protect themselves and, in the event of an incident, recover more quickly.

By taking these reasonable steps, businesses should feel confident enough to experiment with GenAI, rolling out the innovations that are right for them and their clients.

Jaini Gudhka, senior risk manager, QBE Europe

QBE. Prepared.

How can businesses build resilience in a challenging operating environment?

Visit QBEeurope.com/sector-resilience to find out.

QBE
Business insurance