QBE
At the heart of it

# Cloud cover

## Forecasting digital disruption in a cybercrime climate



## Three things to takeaway:

1. How cloud and AI adoption can boost efficiency, but risk greater exposure for businesses.

2. How threat actors are evolving, and using new tools and old tactics to attack and disrupt businesses.

3. How businesses can embed risk management into tech so that resilience is built in, not bolted on, to future planning.

# AI adoption and cloud platform capabilities are transforming business

– but the speed and scale of such a rapid shift provides rich opportunity for ransomware, fraud and third-party disruption.

The shift to public, private and hybrid cloud platforms is unlocking new efficiencies, driving automation and supporting artificial intelligence (AI) adoption. These advances are creating competitive advantages, but they are also unfolding against a threat landscape that is evolving even more rapidly. As businesses increase their reliance on cloud services, attackers are exploiting weaknesses such as poor identity controls, misconfigurations and unsecured data.

Generative artificial intelligence (GenAI) amplifies risk, enabling adversaries to act with greater speed and precision, while lowering the technical barriers for entry-level cybercriminals. With threat actors using GenAI to breach security systems, businesses are exposed to operational disruption, resulting in financial, reputational and potential regulatory impacts. Threats linked to GenAI use have manifested in deepfake± scams, identity fraud and automated phishing† attacks. Ransomware incidents continue to rise as a result, with IT-ISAC recording 1537 ransomware attacks in Q1 2025, compared to 572 in Q1 2024, and the disruption they cause now represents a fundamental risk to organizations dependent on third parties, including cloud providers.

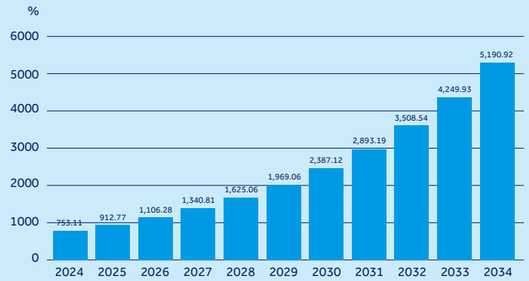
**Glossary**

± **Deepfake:** an AI-based technology used to produce artificial video or audio content that appears convincingly lifelike.

† **Phishing:** an attempt to obtain private and confidential information from internet users, such as usernames, passwords and credit card details. Cybercriminals typically send emails or contact victims through instant messaging, pretending to be legitimate or official correspondents. These phishing emails or messages often contain links infected with malware.

A proactive, resilience-first approach is essential. Businesses must embed risk management into their technology systems, anticipate third-party vulnerabilities and build continuity planning into their operations.

**Figure 1: Projected value of global cloud computing market by year** (USD billion)




Control Risks Source: Precedence Research[1]

The scale of cloud adoption underscores the urgency in moderating this exposure. The global market is expected to exceed USD 5 trillion by 2034, up from USD 912 billion in 2025.[2] As more organizations transfer infrastructure and data to the cloud servers, those servers become high-value targets. High-severity cloud alerts increased by 235% throughout 2024 compared with the previous year,[3] reflecting both the surge in adoption and the increasing capability of attackers.

Most cloud-hosted attacks focus on business email compromise (BEC).[4] Criminals exploit platforms such as Microsoft 365 to launch BEC phishing campaigns, which can open the door for taking over accounts or harvesting credentials, through a trusted cloud platform rather than via typosquatted‡ domains or email spoofing**. This means these attacks can be completed without triggering many common security measures.[5] Additionally, state-linked threat actors and sophisticated cybercriminal groups are favouring cloud-specific threats to digital infrastructure.

1 precedenceresearch.com/cloud-computing-market
2 precedenceresearch.com/cloud-computing-market
3 unit42.paloaltonetworks.com/2025-cloud-security-alert-trends
4 ibm.com/thought-leadership/institute-business-value/report/2025-threat-intelligence-index
5 guardz.com/blog/sophisticated-phishing-campaign-exploiting-microsoft-365-infrastructure

**Glossary**

‡ **Typosquatting:** the practice of registering commonly misspelled versions of legitimate domain names to spread malware via links in phishing emails or drive-by downloads. For instance, a variant of the legitimate domain example.com might be maliciously registered as exxample.com.

** **Email spoofing:** a tactic where an attacker forges a sender's address in an email to disguise the true origin, making it appear as if it was sent from a trusted source.

## Double exposure: ransomware and phishing

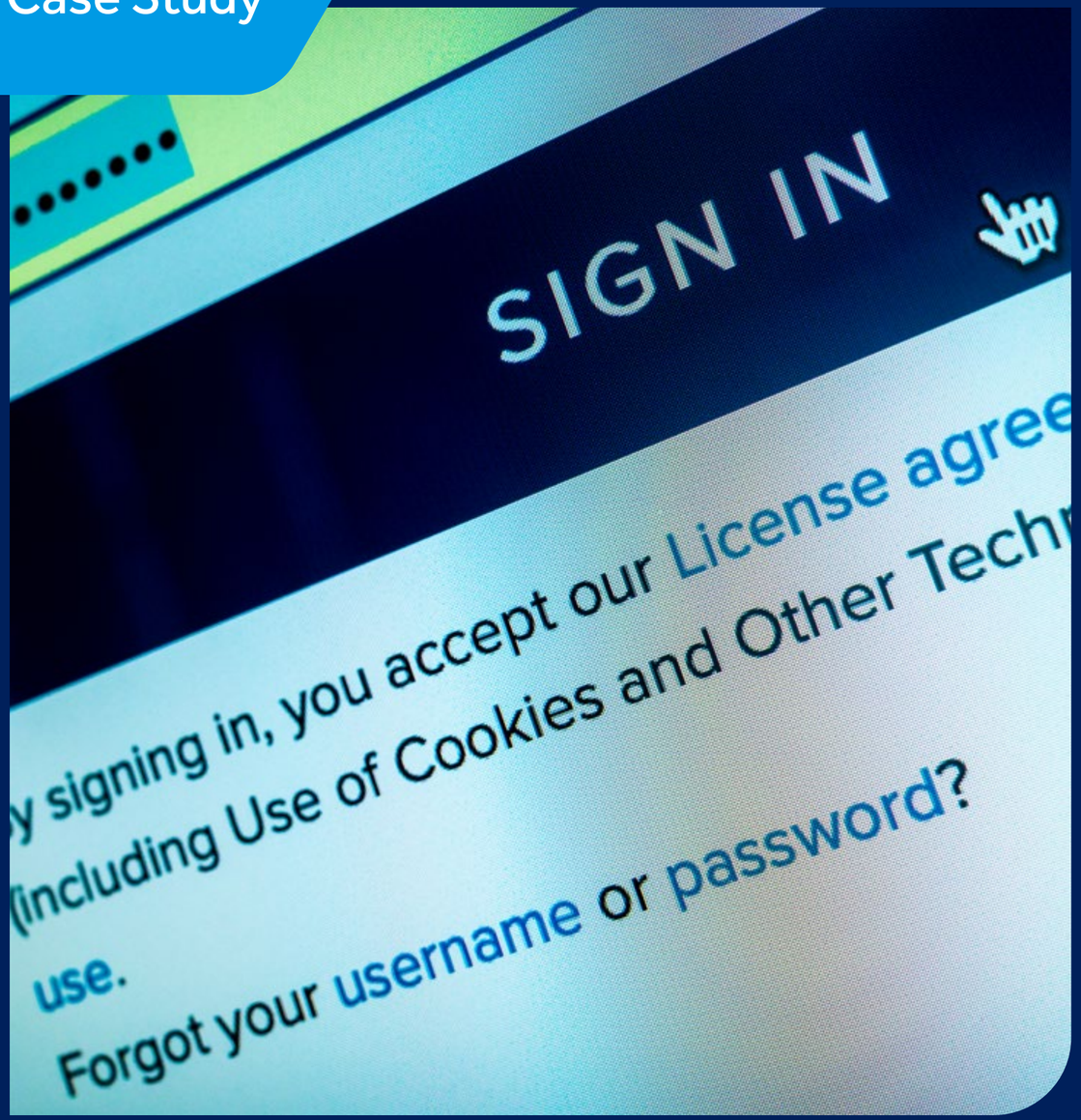
Nearly half of corporate data stored in cloud servers is classified as sensitive,[6] making it attractive to ransomware operators. New ransomware variants are designed to scan for and target cloud-based collaboration tools, and attackers are increasingly able to move laterally between on-premises and cloud systems, encrypting or exfiltrating data as they go.[7]

Phishing remains the leading access point for cloud-related incidents, accounting for one-third of intrusions in 2023 and 2024.[8] Often, attackers leverage phishing tactics to steal credentials through adversary-in-the-middle (AITM) attacks‡. Threat actors have also been successful in exploiting cloud application flaws, using stolen legitimate credentials, and gaining access to privileged users or service accounts.

6 cpl.thalesgroup.com/resources/webinars?commid=615147&bt_tok=%7b%7bRecipient.ID%7d%7d
7 microsoft.com/en-us/security/blog/2024/09/26/storm-0501-ransomware-attacks-expanding-to-hybrid-cloud-environments
8 ibm.com/new/announcements/x-force-cloud-threat-landscape

**Glossary**

‡ **Adversary-in-the-middle (AITM) attack:** also known as man-in-the-middle (MITM) attack, this refers to a threat actor inserting itself between a conversation taking place between the user (victim) and system. The attacker's position allows them to intercept, send and receive data that is meant for one end of the legitimate conversation or is not meant to be sent at all.




## Okta, 2023

Single sign-on (SSO) provider Okta was compromised when unnamed attackers stole credentials and gained access to its support case management system. Sensitive data, including cookies and session tokens, was stolen, enabling impersonation of valid users.

One customer, 1Password – a password manager with over 100,000 business users – detected suspicious activity on their Okta account (used for employee facing apps) on 29 September, when they immediately terminated the activity and investigated.[9] Okta didn't notify 1Password about the breach until 19 October, a full 16 days later, despite another cybersecurity customer, BeyondTrust, alerting Okta to a breach on 2 October.[10]

In total, 134 of Okta's business clients were affected, and Okta suffered a USD 2 billion loss in market value.[11,12]

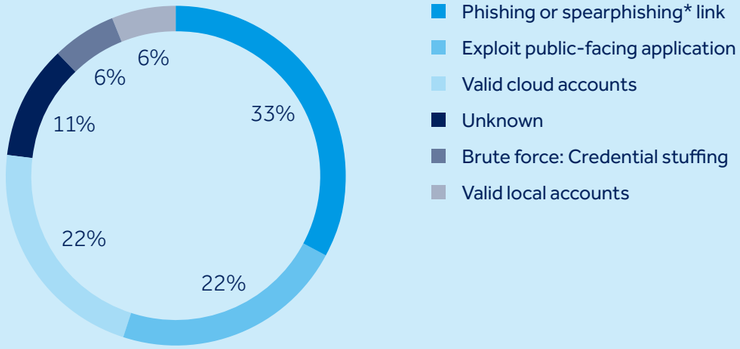
9 arstechnica.com/security/2023/10/1password-detects-suspicious-activity-in-its-internal-okta-account
10 portnox.com/blog/cyber-attacks/unpacking-the-okta-data-breach
11 nightfall.ai/blog/okta-data-breach-what-happened-impact-and-security-lessons-learned
12 cnbc.com/2023/10/23/okta-hack-wipes-out-more-than-2-billion-in-market-cap.html

## Supply chain and third-party dependencies

The growing convergence of data hosting and management has made third-party providers an attractive target for cybercriminals. A single compromised supplier can expose multiple businesses – sometimes hundreds at a time. Cloud and data storage is a likely target for threat actors of all capabilities, as data is growing in value on cybercriminal marketplaces.

By 2025, the volume of data stored worldwide is projected to reach 200 zettabytes (200 trillion gigabytes) across private and public IT infrastructures, utility infrastructures, private and public cloud data centres, personal devices and internet of things (IoT) devices.[13] Half of this data will be stored in the cloud, compared with 43% of data stored in the cloud in 2024[14], an estimated 15% in 2020[15] and only 10% in 2015.[16] This concentration of valuable data makes cloud providers and storage services appealing to attackers.

**Figure 2: Attacks on cloud environments, by initial access vector (2022-24)**




Control Risks – Source: IBM[17]

13 cybersecurityventures.com/the-world-will-store-200-zettabytes-of-data-by-2025/
14 storagenewsletter.com/2023/01/25/43-of-data-to-be-stored-in-public-cloud-by-2024-on-average/
15 gartner.com/en/documents/3989101
16 statista.com/statistics/1062879/worldwide-cloud-storage-of-corporate-data/
17 ibm.com/new/announcements/x-force-cloud-threat-landscape

**Glossary**

* **Spearphishing:** a more targeted form of phishing that focuses on specific groups of people who share a common characteristic. For example, they may work in the same company, attend the same university, use the same financial services or institution, or order from the same websites.

## MURKY PANDA, 2023-present

MURKY PANDA, a prolific nation state-linked threat actor in China, has been observed exploiting zero-day vulnerabilities in software-as-a-service (SaaS) providers to gain access to their network. The group can breach defences to remain undetected in customer systems for extended periods, where they benefit from prolonged access to private data. MURKY PANDA has also compromised a Microsoft cloud solution provider by abusing delegated administrative privileges for IT and technical personnel.[18]

The group presents a serious threat to government, technology and professional services entities in North America, particularly through the compromise of suppliers with access to sensitive information. Cloud environments are extremely vulnerable to MURKY PANDA's advanced capabilities and knowledge of custom application logic to exploit the functionality of applications rather than leveraging technical vulnerabilities.

18 crowdstrike.com/en-us/blog/murky-panda-trusted-relationship-threat-in-cloud

# Nation-state actors

## State-linked groups are increasingly exploiting weaknesses in cloud systems.

### GenAI: defence or weapon?

GenAI is reshaping the cyber threat environment. Its usage and marketplaces look certain to surge over the next five years in North America and Europe as GenAI tools bring productivity benefits across most, if not all sectors.

- ChatGPT has 755m and Microsoft Copilot 88 m active users in 2025.[19]
- ChatGPT users increased by 33% between December 2024 and February 2025.[20]
- 78% of organizations deploy AI in at least one business function in 2025, up from 55% in 2024.[21]
- 20-40% of employees actively use AI in their roles, particularly in programming.[22]

But the misuse of the same technology for fraud and extortion has emerged as a widespread threat. Deepfake-enabled fraud is a particularly alarming development, where cybercriminals impersonate executives, board members and public figures using synthetic voices, videos and images.

These tactics are employed to deceive employees into transferring substantial sums of money to unauthorized accounts controlled by criminal networks. In 2024, deepfakes were implicated in nearly 10% of successful cyberattacks, with financial losses ranging from USD 250,000 to more than USD 20 m.[23]

19 firstpagesage.com/seo-blog/chatgpt-usage-statistics
20 demandsage.com/chatgpt-statistics
21 sqmagazine.co.uk/ai-tools-usage-statistics
22 sqmagazine.co.uk/ai-tools-usage-statistics
23 Control Risks


## Unnamed Singapore company, 2024

An employee of a multinational company in Singapore was deceived by a fraud actor impersonating the CFO. Believing the video call to be genuine, the employee authorised a transfer of nearly USD 500,000.[24] Although the money was traced and withheld by Singapore and Hong Kong police forces, the incident likely resulted in significant response and remediation costs.

24 channelnewsasia.com/singapore/deepfake-scam-impersonate-ceo-company-finance-director-5048706

State-sponsored attackers also use GenAI to write malicious code, using large language models (LLMs) to conduct reconnaissance and scale malware operations. Such actors may also target LLMs used by businesses for internal functions downstream, causing outages and integrity issues that disrupt operations.

Cybercriminal groups have increasingly leveraged GenAI and deepfake technologies to conduct financially motivated attacks across sectors on a global scale. GenAI is capable of crafting effective phishing templates or conducting highly sophisticated social engineering campaigns at speed. Low-capability cybercriminal attackers have used AI to assist in script development and malware coding.[25] Businesses will likely face a rise in attacks from groups previously dismissed as too technically incompetent or resource-poor to pose a realistic threat.[26] Ransomware extortion cases that were publicly disclosed increased by 54% in January-April 2025 compared with the same period the year before.[27]

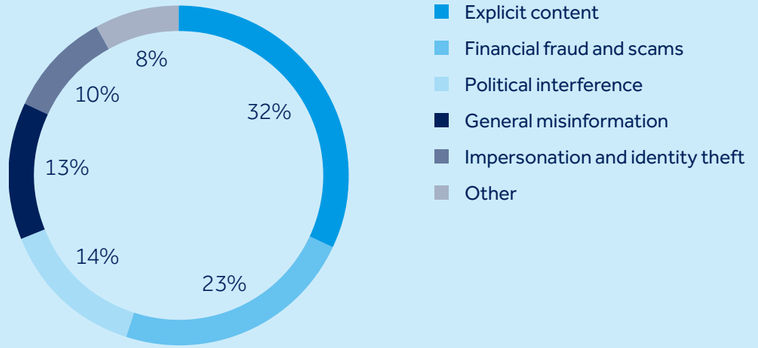
25 hp.com/us-en/newsroom/press-releases/2024/ai-generate-malware.html
26 anthropic.com/news/detecting-countering-misuse-aug-2025
27 Control Risks

## Amazon, 2025

A white-hat hacker highlighted critical weaknesses in Amazon's Q extension for Visual Studio Code by submitting a malicious pull request. Using only an unprivileged GitHub account, the hacker was inadvertently granted administrative-level credentials. This access allowed them to instruct the assistant to reset to factory default settings, wipe local file systems and delete cloud resources databases. The attacker, who described the exercise as exposing Amazon's "AI security theatre", needed no sophisticated malware to succeed – underscoring weaknesses in third-party security architecture and controls.[28] Although no sensitive data was destroyed, the incident could inspire similar attacks on Amazon's security and AI-enabled assistance services.

28 404media.co/hacker-plants-computer-wiping-commands-in-amazons-ai-coding-agent

**Figure 3: Content type of deepfake attacks, Q1 2025**




Control Risks – Source: Resemble AI[29]

## The cost of compromise

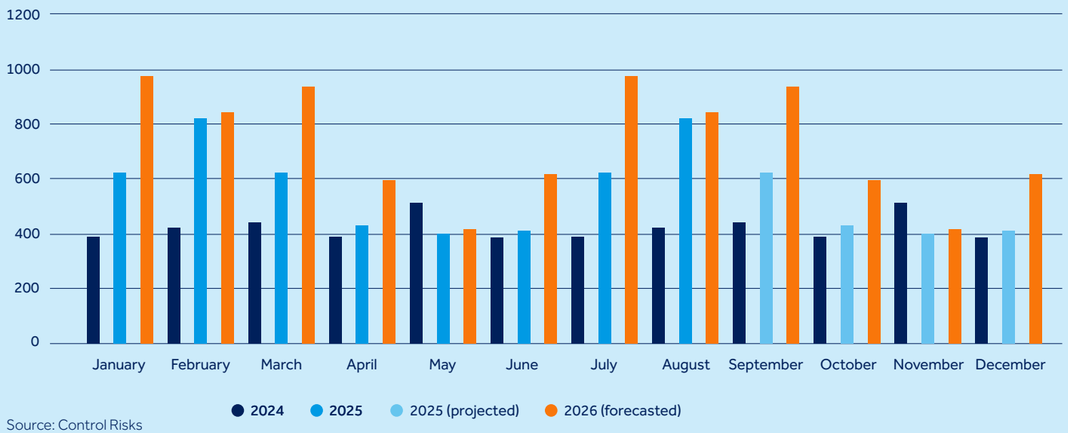
Successful ransomware attacks can trigger financial losses, reputational harm and even litigation, not only for the targeted business, but also for third-party providers and their customers. The widespread adoption of cloud services and other emerging technologies has coincided with a steady rise in ransomware activity in recent years. A major wave of attacks against organizations in the UK retail and finance sectors in May 2025, led by cybercriminal group Scattered Spider, highlights this pattern. The group relied on advanced social engineering and phishing to gain entry, impersonating trusted platforms through typosquatted domains of third-party SaaS providers and phishing kits that tricked victims into handing over credentials and session data.[30]

29 resemble.ai/wp-content/uploads/2025/04/ResembleAI-Q1-Deepfake-Threats.pdf
30 reliaquest.com/blog/scattered-spider-cyber-attacks-using-phishing-social-engineering-2025

Organizations worldwide continue to face significant disruption from third-party failures. Over the past two years, mass outages and cyber incidents originating from suppliers have affected multiple sectors. One of the most notable was CrowdStrike's faulty update to its Falcon Sensor in 2024, which impacted around 8.5 m Windows devices. While this represented fewer than 1% of all Windows machines, the outage had global consequences, with healthcare, aviation and other transport among the hardest hit sectors.

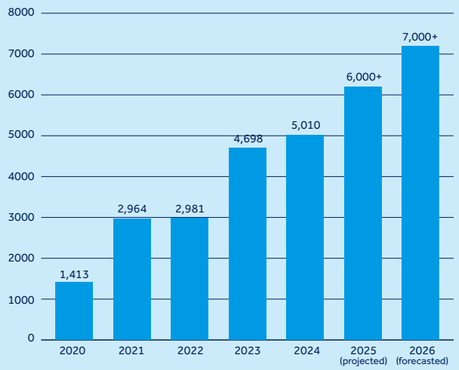
Cybercriminals quickly exploited the situation, launching follow-up phishing campaigns that used CrowdStrike-related lures to compromise systems, steal data and extort victims. Although the incident was not a targeted attack, it highlighted the systemic impact such failures can have on organizations reliant on SaaS for critical business functions. Previous attacks, such as the MOVEit mass vulnerability campaign and the NotPetya mass cyber attack, demonstrated similar ripple effects, disrupting downstream customers well beyond the original point of compromise.

## Figure 4: Projected monthly numbers of ransomware victims named on data leak sites



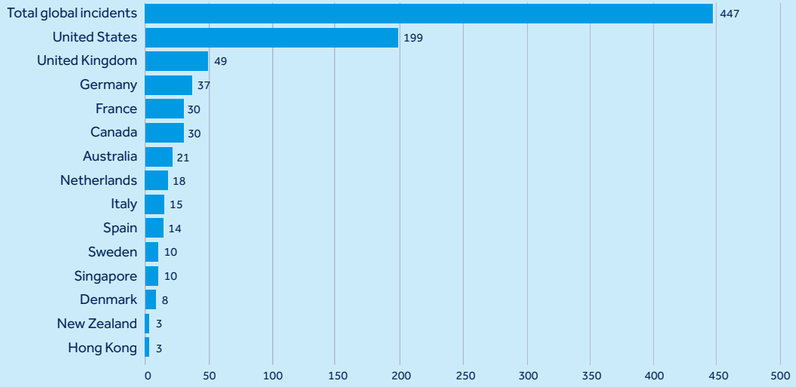

Source: Control Risks

## Figure 5: Total number of ransomware victims named on leak sites (globally)




Source: Control Risks

## Figure 6: Number of significant cyber incidents recorded by geography (August 2023-August 2025)



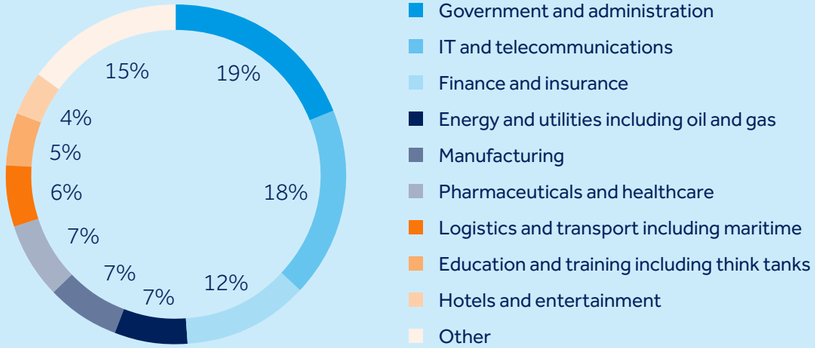

Source: Control Risks

## Rackspace, 2022

In 2022, the Play ransomware group disrupted Rackspace's Hosted Exchange email service by exploiting a zero-day privilege escalation vulnerability in Microsoft Exchange. At least 27 Hosted Exchange customers were affected after the attackers gained initial access through compromised credentials, cutting off email access across their organizations.[32] The fallout was significant: Rackspace was forced to discontinue its Hosted Exchange service, faced multiple customer lawsuits and was alleged to have incurred losses of around USD 11 m.[32]

31 ir.rackspace.com/news-releases/news-release-details/update-recent-cybersecurity-incident
32 msspalert.com/news/rackspace-taking-losses-of-roughly-11-million-for-hosted-exchange-ransom-attack

**Figure 7: Cyber incidents affecting key markets, by sector**
(August 2023-August 2025)




Source: Control Risks

Globally, organizations face the growing risks of operational downtime, financial loss and reputational damage as criminals exploit an expanding attack surface. The increasing use of third-party services such as cloud-hosting, external software or AI tools in day-to-day operations has given threat actors more opportunities to strike.

# Resilience by design

If cloud adoption and AI integration accelerate at the expected pace, attackers will continue to benefit from increased opportunities and entry points, and businesses will remain vulnerable to attack. A robust strategy is essential to anticipate and withstand cyber incidents, particularly those arising from third-party services and cloud environments that now underpin critical business functions.

Building resilience means embedding cyber risk management into technology lifecycles from the outset. This involves implementing strong identity and access management (IAM) protocols, running regular configuration audits, and encrypting sensitive data across all cloud environments. Proactive measures such as continuous monitoring, threat intelligence, and incident response plans help detect and contain threats before they escalate.

Businesses should also evaluate the security posture of their third-party providers and establish clear protocols for managing supply chain exposure. By adopting these practices together, organizations will better protect operations, preserve continuity and maintain trust in an increasingly volatile cyber landscape.

Building resilience means embedding cyber risk management into technology lifecycles. This involves strong identity and access management protocols, regular configuration audits, and sensitive data encryption.

## Microsoft Azure, 2024

In July 2024, a distributed denial-of-service (DDoS) attack disrupted Microsoft's Azure cloud platform, knocking services offline for up to eight hours. The disruption was caused by a surge in usage affecting Azure Front Door and Content Delivery Network. Then a failure in defensive implementation amplified the impact rather than containing it.[33]

33 forbes.com/sites/kateoflahertyuk/2024/07/31/microsoft-confirms-new-outage-was-triggered-by-cyberattack

# Steps to building cyber resilience

Mature organizations can build proportionate cyber resilience through several actions:

**Understand and index risk profiles** to identify critical assets, threats, and vulnerabilities and document a clear view of organizational exposures.

**Define acceptable organizational risk** so leadership sets clear boundaries for acceptable risk and exposure.

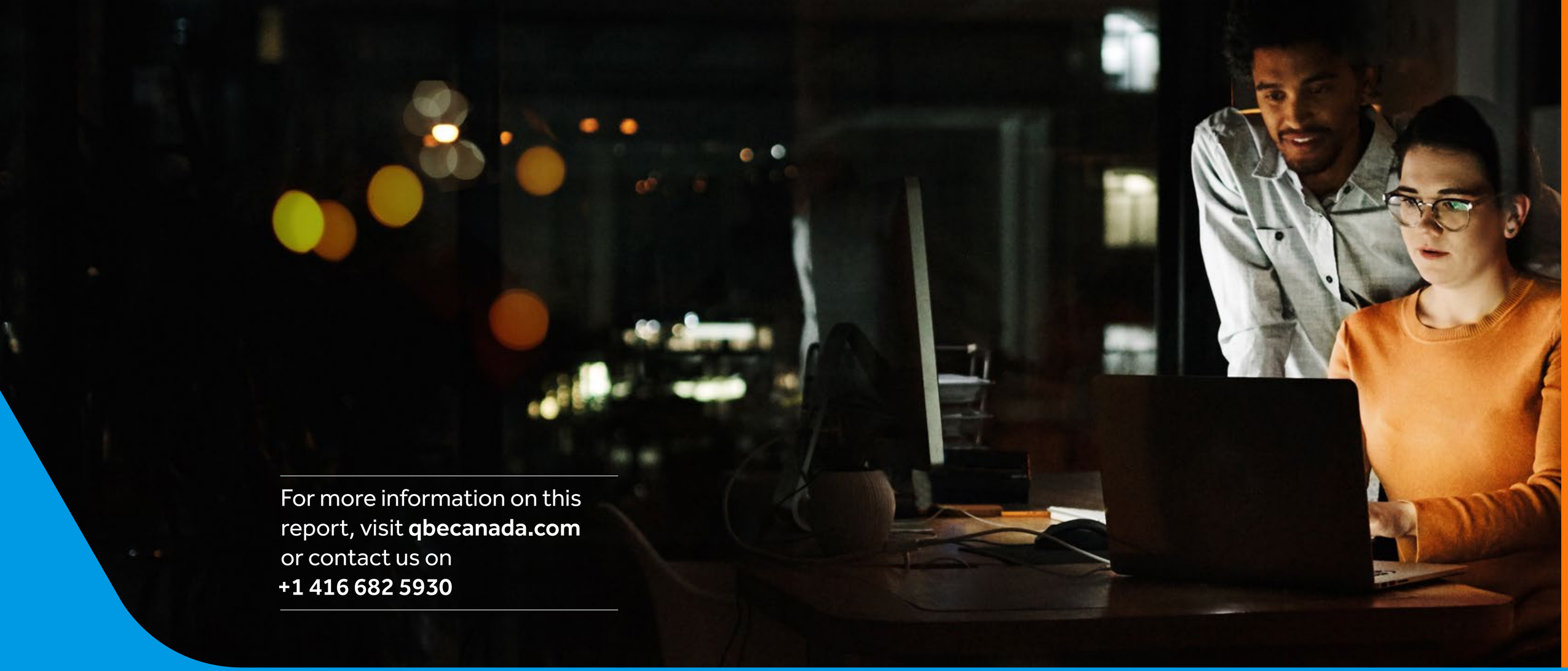
**Prioritize risk mitigation strategies** that focus resources where they will have the greatest impact.

**Prepare for worst-case scenarios** with tested contingency plans and recovery protocols.

**Test crisis management capabilities** to stress test decision-making, communication, and crisis response.

**Integrate third-party support into cyber security strategy** to provide expertise on managing residual risks.

**Proactively monitor trends and adapt** cyber defences to stay ahead of evolving threats, new technologies and changing business needs.



For more information on this report, visit **qbecanada.com** or contact us on **+1 416 682 5930**


**Toronto**
6 Adelaide St. E
7th Floor
Toronto, ON M5C 1W4
Canada
+1 416 682 5930

**QBEcanada.com**

**Vancouver**
1021 West Hastings Street
Suite 1570
Vancouver, BC V6E 0C3
Canada
+1 604 558 5729



This report was produced by QBE with Control Risks

**QBE Services Inc.**
Registered office: 6 Adelaide St. E, 7th Floor, Toronto, Ontario M5C 1W4
Registered in the Province of Ontario, Canada No. 002193827


QBE
At the heart of it

995271/2510-CAN