TOKIO MARINE
HCC

Top 10 Cyber Incidents 2024

Top 10 Incidents 2024

2024 has been marked by an alarming rise in supply chain attacks, a trend that has captured the attention of cyber security professionals these past years. These incidents have demonstrated how vulnerabilities in interconnected systems can cascade through organisations, causing widespread disruption. As businesses continue to rely on shared infrastructure, the need for robust collaboration and proactive security measures has become increasingly evident.

At the same time, the growing complexity of software provider supply chains has exposed weaknesses in widely used cloud environments and enterprise software solutions. Incidents such as the ones involving CrowdStrike, Change Healthcare, CDK Global or Blue Yonder have showcased the critical importance of implementing adequate security strategies to protect these ecosystems.

Looking forward, the events of this year highlight the necessity of balancing innovation and resilience. Organisations must prioritise not only technological advancements but also the frameworks needed to mitigate the security risks in a globally connected world. 2024 serves as a pivotal moment to reassess the strategies that will shape the future of cyber security.

This year's top 10 report highlights some of the most important incidents of 2024 that have shaped the cyber landscape. It is not a ranking but rather shows a list of incidents that have caused widespread disruption and/or had a significant financial impact.

CrowdStrike

1

(Information security software provider)

SOURCE 1
SOURCE 2
SOURCE 3

Impact

A global IT Outage caused one of the largest disruptions in IT history, affecting 8.5 million devices globally, leading to financial losses of approximately US$5.4 billion. Airlines, healthcare, and finance sectors were significantly disrupted.

On 19 July, CrowdStrike, a cyber security company, distributed a faulty update to its Falcon Sensor security software, causing widespread crashes (showing the infamous Blue Screen of Death) on Windows systems that were running it.

Despite the error being discovered and a fix released by CrowdStrike a few hours later, many affected systems had to be fixed manually, and organisations faced prolonged recovery times.

Change Healthcare

2

(Healthcare software provider)

SOURCE

Impact

This was a ransomware attack that resulted in a massive disruption in the US healthcare system lasting several weeks. It compromised the protected health information of at least 100 million individuals (almost one-third of the population of the US). The cost of the attack rose to US$4.457 billion.

On 21 February, Change Healthcare publicly disclosed that it had been impacted by a cyberattack. They were hit with a ransomware attack from the well-known threat actor group BlackCat or ALPHV, disrupting key operations that resulted in massive disruption in the US healthcare system for weeks.

Change Healthcare, in response to the ransomware attack, shut down more than 111 different services to prevent further damage, which prevented many pharmacies and hospitals, as well as other healthcare facilities and offices, from processing claims and receiving payments. After almost one month, on 18 March, they claimed to have successfully reinstated 99% of their pharmacy network services.

CDK Global

3

(Automotive software provider)

SOURCE

Impact

This was a ransomware attack that caused a massive outage of car dealerships' core software.

On 18 June, CDK Global – a company that provides SaaS-based CRM, payroll, finance and other key functions for car dealerships around North America (nearly 15,000 dealership locations) – was hit by a ransomware attack.

The attack forced CDK Global to shut down its systems, phones and applications to contain the threat and prevent further damage. Just as recovery efforts began, a second breach occurred, intensifying the disruption of the software provider's operations, and impacting all dealership services reliant on their systems.

Israel – Hamas war

4

(Nation-state attack)

SOURCE

Impact

This kinetic cyber attack caused direct and indirect physical damage.

The ongoing conflict between Israel and Hamas continues to escalate, with no clear resolution in sight. Tensions remain high as both sides engage in retaliatory action. Amid rising tensions, recent incidents have further intensified the situation.

On 17 September, paging devices used by Hezbollah forces in Lebanon and Syria exploded. The following day, walkie-talkie devices exploded all over Lebanon. These incidents are widely attributed to Israel, leaving more than 30 dead and 3,200 injured.

RegreSSHion

5

(IT software provider)

SOURCE 1

SOURCE 2

Impact

This zero-day incident that affected over 7 million exposed instances of OpenSSH servers.

On 1 July, a new critical vulnerability was discovered in OpenSSH servers affecting glibc-based Linux systems.

The RegreSSHion vulnerability (CVE-2024-6387) was a critical signal handler race condition that affected OpenSSH's server (sshd) versions and potentially resulting in unauthenticated remote code execution (RCE) with root privileges.

According to Palo Alto data, over 7 million exposed instances of OpenSSH versions 8.5p1-9.7p1 were seen globally as of 1 July. Including older versions (4.3p1 and earlier), the total increased to 7.3 million instances.

6 XZ Utils

(IT software provider)

SOURCE 1

SOURCE 2

Impact

This critical vulnerability constituted a near miss in software supply chain security.

On 29 March, a Microsoft software engineer uncovered a critical vulnerability in the widely used open-source library XZ Utils (and its underlying library liblzma). The weakness, identified as CVE-2024-3094, had a CVSS score of 10 and involved an SSH backdoor that would allow remote, unauthenticated attackers to achieve remote code execution.

The discovery of this vulnerability was purely accidental but revealed a sophisticated and long-term operation that was suspected to be carried out by a state-sponsored actor even though no specific attribution currently exists. The attacker had begun contributing to the XZ Utils project as early as February 2022. Over time, they built sufficient trust within the community to gain maintainer privileges, which they then exploited to introduce the backdoor.

Fortunately, the malicious code was detected before it was widely distributed, averting what could have been a catastrophic software supply chain attack with global implication in Linux Operating systems. The incident highlights the importance of strengthening security checks and monitoring within open-source software ecosystems.

7 Ivanti VPN attacks

(IT software provider)

SOURCE 1

SOURCE 2

Impact

Severe compromises in secure remote access of a leading global IT company were uncovered.

Over the course of January and February, several critical vulnerabilities were discovered in Ivanti's Connect Secure and Policy Secure VPN gateways. These weaknesses included authentication bypass and command injection vulnerabilities, enabling attackers to bypass access controls, execute arbitrary commands, and compromise sensitive enterprise systems.

Ivanti is a leading global IT company offering enterprise service management solutions, network and endpoint security, asset management and supply chain management, among others. The widespread adoption of Ivanti's VPN solutions across industries heightened the potential impact, creating substantial risks for supply chains and critical infrastructure.

8 Salt Typhoon

(Critical telecommunications infrastructure)

SOURCE 1

SOURCE 2

SOURCE 3

Impact

This was a large-scale infiltration of critical telecommunications infrastructure with global implications.

During 2024, it was publicly disclosed that, Salt Typhoon, a Chinese state-sponsored hacking group, orchestrated an unprecedented cyber-espionage campaign targeting critical telecommunications infrastructure in the United States and beyond. Exploiting vulnerabilities in network devices such as routers and switches, the attackers infiltrated major providers, including AT&T, Verizon, T-Mobile, and Lumen Technologies.

The attackers employed advanced tactics, such as living-off-the-land techniques and deploying modular malware, to evade detection while gaining persistent access. Notably, the campaign targeted surveillance portals used by law enforcement and intelligence agencies, potentially exposing sensitive operations. Intentionally, the campaign extended to telecom operators in Europe and Asia, demonstrating a global supply chain threat to critical telecommunications infrastructure.

Despite the ongoing remediation efforts, including guidance from CISA and other agencies, the full extent of the damage remains unclear. This event highlights the urgent need for proactive measures to secure critical infrastructure against advanced persistent threats.

Blue Yonder

9

(Supply chain management software provider)

SOURCE 1

SOURCE 2

Impact

This ransomware attack resulted in significant disruptions to retail and grocery supply chains, affecting operations in both the US and the UK.

On 21 November, Blue Yonder, a leading provider of supply chain management software, suffered a ransomware attack that severely impacted its managed services hosted environment. This breach disrupted services for several high-profile customers, including major US grocery retailers like Albertsons and Kroger, and UK-based chains like Sainsbury's and Morrisons. The attack caused delays in deliveries, inventory management issues, and disruption in payment systems, particularly impacting operations during the peak holiday shopping season.

Although Blue Yonder confirmed the attack and was working with external cyber security firms, the company was unable to provide a timeline for full restoration. Notably, Starbucks also reported operation issues, including difficulties in employee payment and scheduling across 11,000 stores in North America.

The Termite ransomware group later claimed responsibility for the attack, although the company did not confirm data theft, instead focusing on recovering disrupted services. This incident highlights, once more, the growing threat ransomware poses to companies integrated deeply into global supply chains.

Snowflake

10

(Cloud software provider)

SOURCE 1

SOURCE 2

Impact

This was an extensive data breach that compromised customer data across numerous industries, including finance, retail and technology.

On 31 May, Snowflake, a leading cloud data storage platform, was compromised in a cyberattack that exposed sensitive customer data from several high-profile companies. The attackers, leveraging stolen credentials obtained via infostealer malware, gained unauthorised access to Snowflake customer environments. This breach affected a broad range of organisations, including Ticketmaster, Santander, Mitsubishi, and Progressive.

This attack was primarily driven by poor security practices, including the use of single-factor authentication and unsecured demo accounts. Snowflake later confirmed that no breach occurred within their core platform or systems but that the attackers exploited weak authentication mechanisms in customer environments to steal data. The breach resulted in the exposure of sensitive data, including account numbers, credit card details, and HR information.

Although Snowflake denied that its own systems were directly breached, the incident exposes significant weaknesses in how cloud services are used by businesses and highlights the importance of robust authentication and access controls.

Bonus Track

1 The evolving cyber security landscape: Lessons from the CrowdStrike incident

Risk accumulation on cloud providers

As organisations increasingly rely on a handful of dominant cloud providers, such as AWS, Microsoft Azure, and Google Cloud, the market for public cloud services has become highly concentrated. This consolidation introduces systemic risks, where disruptions or vulnerabilities within a single provider can ripple across entire industries. The distribution of market share among these providers illustrates the extent of this dependency and highlights the importance of strategies to mitigate potential risks from such concentrated reliance.

Cloud provider	Market share (2023)
Amazon	39.0%
Microsoft	23.0%
Google	8.2%
Alibaba Group	7.9%
Huawei	4.3%
Others	17.6%
Total	100%

The increasing reliance on a small number of cloud providers to host workloads, data, and critical infrastructure introduces:

- **Operational interdependence:** Cloud providers host not only individual companies but also the platforms and software ecosystems that support global supply chains.
- **Geopolitical risks:** The dominance of US-based providers raises concerns about data sovereignty and potential exposure to sanctions or export restrictions in cross-border operations.
- **Single point of failure and ripple effect:** A failure or breach in a leading cloud provider can disrupt thousands of dependent services simultaneously.

The following strategies can help mitigate the risks that the extensive use of cloud providers may pose to companies:

- **Multi-cloud strategies:** Diversifying workloads across multiple providers to reduce exposure.
- **Edge computing:** Shifting some workloads closer to end users to distribute dependency and improve bandwidth availability.
- **Vendor due diligence:** Ensuring cloud providers maintain high resilience and transparency standards.

EDR diversification as strategy

The CrowdStrike outage highlighted the risks of relying exclusively on a single Endpoint Detection and Response (EDR) solution. Implementing EDR diversification aims to achieve:

- **Redundancy:** Adopting multiple EDR providers ensures that if one vendor experiences disruption, the backup system can maintain endpoint protection and minimise downtime.
- **Improved threat detection:** Using diverse tools increases the likelihood of detecting sophisticated threats that evade a single provider's algorithms.

However, it also introduces several challenges:

- **Complexity management** in integrating alerts and managing overlapping tools.
- **Increased operational cost** due to maintaining multiple licenses, training staff on multiple systems, and managing extra alerts.

While implementing EDR diversification could have mitigated the impact of a global IT outage like the CrowdStrike incident, it is not a one-size-fits-all strategy. Organisations must carefully assess their unique risk exposure, operational capacity and resource availability before adopting this approach. Ultimately, the decision requires balancing the benefits of resilience with the challenges of complexity to align with broader cyber security and business goals and priorities.

On-premises data centres: back to basics?

In certain scenarios, organisations are reconsidering on-premises data centres due to specific risks and operational demands. While cloud solutions dominate for scalability and flexibility, on-premises data centres offer unique advantages in strategic cases:

- **Risk reduction:** By maintaining critical infrastructure on-premises, organisations seek to minimise exposure to geopolitical conflicts, third-party failures, or supply chain dependencies.
- **Cost efficiency:** The associated costs of the scalability of cloud solutions can increase unpredictably as usage grows, especially for compute-intensive workloads or massive storage needs (e.g., Artificial Intelligence). On-premises data centres, though requiring significant upfront investments, could offer more predictable long-term costs and greater control over infrastructure expenses. For large enterprises, retaining legacy systems can sometimes be more cost-effective than migrating to cloud.
- **Control and ownership:** On-premises data centres allow organisations to secure intellectual property, crypto assets and sensitive data while following localisation strategies to meet unique operational demands and ensure compliance with regional laws.
- **Legal and compliance:** On-prem environments simplify compliance with complex regulatory requirements, especially in industries like finance and healthcare, and address strict data sovereignty laws (e.g., GDPR or NIS2 directive in Europe).
- **Compatibility:** Certain industries like manufacturing or energy, rely on Operational Technology (OT) and/or Internet of the Things (IoT) systems that pose incompatibilities with cloud platforms.

Organisations should evaluate hybrid models, combining cloud flexibility with on-premises control for critical workloads. For instance, storage-intensive AI training models or compliance-critical healthcare data could remain on-premises, while scalable workloads leverage the cloud.

2 Conclusion

The evolving cyber security landscape of 2024 highlights the need for businesses to adapt their strategies to meet emerging challenges. Incidents like the CrowdStrike outage and supply chain attacks have highlighted the vulnerabilities of over-reliance on cloud providers and single-point solutions. Organisations should prioritise diversification, whether through multi-cloud strategies, hybrid infrastructure models, or EDR redundancy, to build resilience against systemic risks.

Ultimately, the path forward requires striking a balance between scalability, cost efficiency, and control. By tailoring strategies to their unique risk profiles and operational demands, businesses can mitigate the complexities of modern cyber security while safeguarding their critical assets and ensuring long-term stability.

Bibliography:

Source: Gartner. **Worldwide IaaS Public Cloud Services Revenue Grew 16.2% in 2023** (July 2024)

https://www.gartner.com/en/newsroom/press-releases/2024-07-22-gartner-says-worldwide-iaas-public-cloud-services-revenue-grew-16-point-2-percent-in-2023

Source: S&P Global Market Intelligence. **2024 Trends in Datacenter Services & Infrastructure** (2024)

https://pages.marketintelligence.spglobal.com/EMC-231115-PC-GL-TMT-RASS-451R-CIQPro-2024TopTMTTrends_06-DatacenterSvcsandInfrastructure-Thankyou.html

Source: Mckinsey. **Investing in the rising data center economy** (January 2023)

https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/investing-in-the-rising-data-center-economy

Source: Gartner. **Market Share Analysis: Infrastructure as a Service, Worldwide, 2023** (2023)

https://www.gartner.com/document/5539195

Source: **One EDR vs. Multiple EDR: Effective Detection and Response** (June 2024)

https://www.danbrown.co/effective-detection-and-response/

Source: Cloudflare. **What is Data sovereignty?**

https://www.cloudflare.com/learning/privacy/what-is-data-sovereignty/

Source: HPE. **AI Storage**

https://www.hpe.com/uk/en/what-is/ai-storage.html

Source: Medium. **Is it Time to Reconsider On-premises Data Centers?**

https://medium.com/@manikolbe/is-it-time-to-reconsider-on-premises-data-centers-f57e02cebff9

Cyber at Tokio Marine HCC

Tokio Marine HCC has been innovating in Cyber Liability Insurance worldwide, for over 20 years. Our dedicated global team is made up of cyber insurance and in-house claims experts with deep industry knowledge and a wealth of cyber security experience. We promote active knowledge exchange, making us a global leader when it comes to cyber risk, while keeping you at the forefront of emerging threats on the ever-evolving cyber landscape.

From offices in the U.S., our cyber team insures US-domiciled businesses, with a focus on the small- to mid-sized segment, as well as individuals concerned with protecting their family, home and privacy from cyber threats.

From Europe and the U.K., our team concentrates on mid- to large-sized businesses domiciled anywhere outside of the U.S. In addition, we leverage our in-house cyber expertise to enhance other Tokio Marine HCC insurance coverages, letting you take on risk with confidence.

Learn more about Cyber at Tokio Marine HCC by visiting tmhcc.com
Follow us on LinkedIn: #TMHCC_Cyber

Contact us

Barcelona
Tokio Marine Europe - Spanish Branch
Torre Diagonal Mar
Josep Pla 2, Planta 10
08019 Barcelona, Spain
Tel: +34 93 530 7300

London
HCC International
Fitzwilliam House, 10 St. Mary Axe
London EC3A 8BF, United Kingdom
Tel: +44 (0)20 7648 1300
Lloyd’s Box 252, Second Floor

Munich
Tokio Marine Europe - German Branch
Rindermarkt 16
80331 Munich, Germany
Tel: +49 89 3803 4640

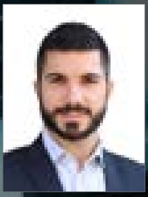
#TMHCC_Cyber

Find out more about our Cyber Security Insurance:

TMHCC Cyber Insurance

Email our Cyber Security Team

This report has been produced by:



Isaac Guasch Garcia
iguasch@tmhcc.com

Isaac Guasch
Cyber Security Leader
Tokio Marine HCC

Marc Pujol
mpujol@tmhcc.com

Marc Pujol
Cyber Security Specialist
Tokio Marine HCC

A member of the Tokio Marine HCC group of companies

Tokio Marine HCC is a trading name of HCC International Insurance Company plc (HCCII), Tokio Marine Europe S.A. (TME) and HCC Underwriting Agency Ltd (HCCUA), members of the Tokio Marine HCC Group of Companies.

HCCII is authorised by the UK Prudential Regulation Authority and regulated by the UK Financial Conduct Authority and Prudential Regulation Authority (No. 202655). Registered with Companies House of England and Wales No. 01575839. Registered office at 1 Aldgate, London EC3N 1 RE, UK. TME is authorised by the Luxembourg Minister of Finance and regulated by the Commissariat aux Assurances (CAA); registered with the Registre de commerce et des sociétés, Luxembourg No. B221975 at 26, Avenue de la Liberté, L-1930, Luxembourg; Operating through its Spanish Branch, domiciled at Torre Diagonal Mar, Josep Pla 2, planta 10, 08019 Barcelona, Spain, registered with the Registro de Entidades Aseguradoras de la Dirección General de Seguros y Fondos de Pensiones under the code E0236, VAT number in Spain (“N.I.F”) W0186736-E, registered with the Registro Mercantil de Barcelona, at volume 46.667, page 30, sheet number B-527127, registration entry 1; and through its German Branch, domiciled at Berliner Allee 26, 40212 Düsseldorf, Germany, registered with the Handelsregister beim Amtsgericht Düsseldorf under the number HRB 84822, authorised by the Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) under the number 5217. VAT ID No: DE320932530. We have authority to enter into contracts of insurance on behalf of the Lloyd’s underwriting members of Lloyd’s Syndicate 4141 which is managed by HCCUA.

The policyholder will always be informed of which insurer in our group will underwrite the policy according to jurisdiction.

Not all coverages or products may be available in all jurisdictions. The description of coverage in these pages is for information purposes only. Actual coverages will vary based on local law requirements and the terms and conditions of the policy issued. The information described herein does not amend, or otherwise affect, the terms and conditions of any insurance policy issued by Tokio Marine HCC Group of Companies. In the event that a policy is inconsistent with the information described herein, the language of the policy will take precedence.