TOKIO MARINE
HCC

Top 10 Cyber Incidents 2025

Top 10 Cyber Incidents 2025

Summary

2025 was marked by a diverse range of cyber incidents that underscored the growing fragility of global digital ecosystems. From disruptive ransomware attacks impacting major retailers and manufacturers to large-scale outages across cloud service providers, the year highlighted how operational, supply-chain and platform dependencies continue to amplify cyber risk. Incidents such as those affecting Marks & Spencer, Jaguar Land Rover, npm's open-source ecosystem and critical telecommunications providers demonstrated how single points of failure can cascade through entire industries.

At the same time, 2025 showed how attackers are rapidly developing their capabilities. The first documented case of an AI-orchestrated espionage campaign illustrated how artificial intelligence (AI) is being leveraged by sophisticated threat actors. This reinforces the need for structured, trustworthy approaches to AI governance.

As always, our Top 10 is not a ranking but rather highlights some of the most important incidents of 2025 that have caused widespread disruption and/or had a significant financial impact.

This year's Bonus Track explores emerging AI risk-management frameworks, with a deep dive into the NIST AI Risk Management Framework, highlighting how organisations can integrate governance, oversight and resilience into their AI strategies.

Together, the incidents of 2025 reflect an increasingly interconnected threat landscape – one that demands proactive, coordinated and adaptive cybersecurity practices.

Marks & Spencer

1

(Retail / consumer goods)

SOURCE

Impact

Large-scale ransomware incident that caused significant disruption across one of UK's largest retailers. Marks & Spencer (M&S) was forced to suspend online ordering, experienced in-store systems outages, and reported the exfiltration of customer personal data. The incident resulted in an estimated £300m impact to operating profit and occurred amid a wider wave of cyber activity affecting the UK retail sector, with other major retailers, including Co-op and Harrods, disclosing cyber incidents during the same period.

On 22 April 2025, M&S publicly disclosed that it had been impacted by a cyberattack. The company confirmed that it faced a ransomware incident that disrupted critical retail operations, forcing the temporary shutdown of online clothing and home orders, and causing interruptions to in-store digital systems, including contactless payments and customer fulfilment services.

As a containment measure, M&S proactively shut down online ordering across its website and mobile app. This had a cascading effect across supply and logistics, delaying deliveries and impacting customer services nationwide. The company later confirmed that the attackers had accessed certain customer data, including names, contact information, dates of birth and order histories, although no financial data or account passwords had been compromised.

The outage lasted several weeks. M&S began restoring operational capabilities gradually, resuming most online clothing deliveries on 10 June, and progressively reinstating click-and-collect, next-day delivery and international shipping in the following days.

During this period, other major UK retailers experienced similar disruptions:

- Co-op confirmed a cyber incident involving the copying of member contact details, which required restricting access to certain internal systems to contain further impact.
- Harrods separately disclosed that a breach at one of its third-party service providers had exposed the personal data of approximately 430,000 customers, again involving contact information but no financial data.

Although these incidents were not officially linked, they occurred within the same timeframe and targeted major UK retail brands, highlighting a broader pattern of coordinated attacks against the retail sector.

Jaguar Land Rover 2

(Automotive manufacturer)

SOURCE 1

SOURCE 2

Impact

Ransomware attack that caused large-scale business interruption, forcing a shutdown of vehicle production across multiple factories for several weeks. According to the Cyber Monitoring Center (CMC) "at £1.9 billion of financial loss, this incident appears to be the most economically damaging cyber event to hit the UK, with the vast majority of the financial impact being due to the loss of manufacturing output at JLR and its suppliers".

On 31 August 2025, British automotive manufacturer Jaguar Land Rover (JLR) detected a cyber intrusion affecting its internal IT and manufacturing systems. As a precautionary measure, in the following days JLR shut down production and key operational networks across major UK facilities to contain the incident and prevent further compromise.

The cybercriminal group Scattered Lapsus$ Hunters claimed responsibility for the attack – a collaboration between Scattered Spider, Lapsus$ and ShinyHunters, three English-speaking threat actors.

The outage halted vehicle assembly, engine production in JLR plants in the UK, Slovakia, China and India, and disrupted dealer and retail operations. This caused significant delays in deliveries and disrupted JLR's wider supply chain. Days later, on 10 September, the company confirmed that the cyberattack also resulted in a data breach affecting some company data. On 25 September, JLR announced a phased restart of its operations, which continued over the following weeks.

AWS, Azure and Cloudflare outages 3

(Cloud infrastructure providers)

SOURCE 1

SOURCE 2

SOURCE 3

Impact

A series of major service outages across Amazon Web Services (AWS), Microsoft Azure and Cloudflare caused widespread disruption to thousands of organisations globally. These events highlighted the systemic risks of cloud concentration, as failures in core components affected critical business applications, online services and customer-facing platforms across multiple industries.

On 20 October, AWS experienced a significant outage originating in the US-EAST-1 region due to a DNS (Domain Name System) resolution failure affecting the DynamoDB endpoint. More than 80 AWS services were impacted, preventing customers worldwide from connecting to cloud-hosted workloads. The disruption lasted approximately 2 hours and 24 minutes, triggering cascading service failures across SaaS providers and digital platforms.

Just days later, on 29 October, Microsoft Azure suffered a global connectivity and DNS outage affecting Azure Front Door, CDN services and authentication processes across multiple regions. The incident caused intermittent failures in application delivery, degraded network performance and login issues for services dependent on Azure. Microsoft later published a post-incident review confirming the root cause to be an internal configuration error.

On 18 November, Cloudflare experienced a large-scale network service disruption after an internal change caused excessive memory consumption in core systems. The outage temporarily affected traffic routing, DNS services and access to a wide range of websites relying on Cloudflare's global edge network. Cloudflare engineers mitigated the issue by rolling back the change and stabilising affected systems.

Although the three incidents were unrelated, their close timing underscored a critical industry concern: a small group of cloud and edge providers is supporting a large portion of global internet infrastructure. As a result, isolated technical failures can rapidly escalate into global service disruption, affecting businesses far downstream from the original issue.

Salesforce / Drift OAuth

4

(IT Software provider)

SOURCE 1

SOURCE 2

SOURCE 3

Impact

A large-scale data breach affecting hundreds of Salesforce customer environments, caused by the compromise of OAuth tokens linked to the Drift/Salesforce integration. The incident enabled unauthorised access to CRM data across multiple organisations, with some security researchers estimating that millions of customer records may have been exposed.

On 21 August, Salesforce issued a security notification regarding the Drift application which integrates with Salesforce via access credentials called OAuth tokens. Days later, in early September, Salesforce customers began reporting suspicious activity linked to their Drift integrations, ultimately revealing a widespread OAuth token breach that enabled the attacker to authenticate into Salesforce customer organisations and extract sensitive CRM data.

Salesforce responded by revoking affected tokens, disabling Drift integrations at scale, and notifying impacted organisations. Several cyber security vendors, including Google's Threat Intelligence team, confirmed that the campaign was carried out by a coordinated threat group (UNC6395) that systematically targeted OAuth-based authorisation flows rather than breaching Salesforce's core platform.

The exposed data varied by organisation but frequently included customer contact details, account information and communication metadata stored in Salesforce objects. There was no evidence that Salesforce's own systems were compromised, with the breach limited to customer environments using the Drift connector.

nmp, Inc.

5

(IT software provider)

SOURCE

Impact

A massive supply-chain attack on the npm ecosystem compromised hundreds of widely used JavaScript packages. The breach injected malicious code into dependencies with billions of weekly downloads, exposing developers' and organisations' environments to credential theft (GitHub tokens, cloud access keys etc.), potential cloud-service compromise, and widespread risk for any project relying on contaminated packages.

On 8 September, attackers initiated a phishing campaign targeting maintainers of popular npm packages. Using compromised maintainer accounts, attackers published malicious versions of critical libraries such as chalk, debug, ansi-styles, and others that are deep in dependency trees.

These malicious versions included a self-propagating worm, publicly dubbed Shai Hulud, which executed upon installation and searched for sensitive credentials stored in environment variables, configuration files, or CI/CD build environments. The worm harvested GitHub Personal Access Tokens, AWS / Azure / GCP credentials, npm tokens and other secrets, exfiltrated them to public attacker-controlled repositories, and then automatically republished infected versions under legitimate maintainer accounts enabling automated lateral spread across the npm registry.

Once discovered, the vulnerability was promptly addressed: on 14 September, registry owners (including GitHub / npm security team) began removing compromised packages and blocking further malicious uploads. By late September, hundreds of packages had been unpublished, and recommendations to rotate credentials, audit dependencies, and purge infected lockfiles were issued to all affected developers.

Oracle Corporation Cloud Platform 6

(Cloud services provider)

SOURCE 1

SOURCE 2

Impact

Alleged large-scale supply-chain breach of Oracle Cloud reportedly affecting over 140,000 tenants, with the threat actor claiming exfiltration of around 6 million records, including encrypted credentials, key files and certificate data.

On 21 March, threat-intelligence firm CloudSEK published a report stating that a threat actor using the alias "rose87168" was offering a dataset of ~6 million records – allegedly exfiltrated from Oracle Cloud's Single Sign-On (SSO) and Lightweight Directory Access Protocol (LDAP) systems – for sale. According to the actor, the breach was achieved via the login endpoint (e.g., login.<region>.oraclecloud.com), exploiting a suspected vulnerability in an old version of Oracle Fusion Middleware (possibly linked to CVE-2021-35587) that allowed full takeover of the authentication infrastructure.

The leaked data reportedly includes a mix of sensitive credentials: encrypted SSO passwords, hashed LDAP credentials,Java KeyStore (JKS) files, private key material, and other authentication artifacts – all of which, if decrypted or misused, could enable malicious access or impersonation across multiple tenant environments globally.

Following the disclosure, the threat actor demanded ransom to suppress resale of the data and offered decryption support for exposed credentials. In public responses, Oracle denied that any breach had occurred, asserting that "published credentials are not for the Oracle Cloud" and that "no Oracle Cloud customers experienced a breach or lost any data."

Nevertheless, independent cyber security vendors and a number of affected organisations reportedly confirmed that elements of the dataset matched real production tenants, generating a widespread concern about cloud infrastructure supply chain exposures and prompting urgent calls for credential rotation, audit of SSO/LDAP configurations, and re-examination of patching policies for legacy middleware.

APT group AI-orchestrated campaign 7

(Cyber-espionage)

SOURCE 1

SOURCE 2

Impact

A state-sponsored cyber-espionage campaign using Claude AI led to a large-scale autonomous attack targeting around 30 global organisations, including tech firms, financial institutions and government agencies. The campaign reportedly automated up to 80–90% of the intrusion lifecycle, marking what Anthropic, the AI company behind Claude, calls the first known AI-orchestrated cyberattack at scale.

In mid-September, security researchers at Anthropic detected a sophisticated espionage campaign attributed to a Chinese state-sponsored APT (Advanced Persistent Threat) group, designated GTG-1002, which leveraged Claude in an "agentic" fashion, i.e., using AI not just as a tool, but as an autonomous agent orchestrating much of the attack.

According to Anthropic, Claude-based agents executed many of the phases of the attack (scanning for vulnerabilities, writing and deploying exploit code, attempting privilege escalation, harvesting credentials and exfiltrating data) across dozens of targets globally.

The intrusion reportedly succeeded in a "small number of cases," with exfiltration of internal data from some victims. Following the disclosure, Anthropic and various cyber security vendors alerted the community, urging organisations to strengthen defensive controls, especially around AI-agent usage, credential management and detection of automated intrusions.

8

SK Telecom

(Telecommunications / Mobile)

SOURCE

Impact

A major cybersecurity breach at South Korea's largest wireless telecom operator SK Telecom exposed personal and USIM-authentication data of approximately 27 million subscribers, creating widespread risk of SIM-cloning, identity theft, and long-term privacy and security consequences. The incident triggered regulatory penalties, mandatory USIM-replacement offers to all customers, and a nationwide security overhaul.

On 18 April, SK Telecom detected abnormal outbound traffic suggesting data exfiltration and reported the breach to authorities two days later. Subsequent forensic analysis uncovered multiple malware families (including BPFDoor, TinyShell and CrossC2) across dozens of servers, with evidence showing that attackers had maintained undetected access since June 2022.

The intrusion resulted in the compromise of data linked to USIM cards, including IMSI and authentication keys, device identifiers, phone numbers and subscriber metadata. This exposure placed nearly 27 million users at risk of SIM-cloning, identity fraud and unauthorised account access.

In response, the South Korean Ministry of Science and ICT (MSIT) launched a Public-Private Joint Investigation Team on 23 April to assess the full scope of the breach, reviewing more than 42,000 servers. By July, regulators ruled SK Telecom negligent and imposed remediation measures, including mandatory quarterly audits, enhanced executive oversight of data security, and a nationwide program for USIM replacement, along with waived cancellation fees for affected customers.

9

Kering Group

(Retail / Luxury goods)

SOURCE 1

SOURCE 2

Impact

A cyberattack affecting several of Kering's luxury-brand houses (including Gucci, Balenciaga and Alexander McQueen) exposed personal information of potentially millions of customers globally. Data reportedly compromised includes names, email addresses, phone numbers, home addresses, and in some cases store-spending histories.

In June, Kering confirmed that an unauthorised third party had temporarily accessed internal systems belonging to some of its brands, marking the discovery of the breach. Hackers identifying as ShinyHunters claimed responsibility, posting samples of the stolen data and alleging that they held more than 7 million customer records. These samples included personal contact information and metadata about customer purchases, including total spend per customer at luxury stores.

Kering notified regulators and affected customers under applicable data protection laws. The company also clarified that the breach did not involve payment information or government issued identity documents. According to its statement, the exposure was limited to personal and contact data from a subset of its brands.

Asahi Group Holdings 10

(Beverages / Manufacturing)

SOURCE 1

SOURCE 2

Impact

Ransomware attack that disrupted Asahi's order processing, shipment operations and call-centre services across Japan. The incident caused nationwide delays in product distribution and raised concerns about potential shortages during peak demand periods.

On 29 October, Asahi Group Holdings detected a cyberattack that forced the company to suspend key operational systems across its manufacturing and logistics network in Japan. As a precautionary measure, Asahi shut down parts of its IT environment to contain the intrusion, resulting in halted order processing, delays in shipments and the temporary outage of call-centre support.

The ransomware group Qilin later claimed responsibility for the attack, although Asahi did not confirm the extent of data compromise. The operational impact was immediate: beverage deliveries across Japan were disrupted, retailers reported delays in stock replenishment, and some distribution centres temporarily paused activity while Asahi worked to restore systems safely.

In the following days, Asahi initiated phased recovery efforts, leveraging backup environments and external cyber security partners to rebuild affected systems. While production facilities remained operational, the company warned of ongoing distribution delays. Regulators were notified and Asahi committed to strengthening security controls across its manufacturing and supply chain infrastructure.

Bonus Track

AI Risk Management Frameworks

Artificial intelligence (AI) has rapidly shifted from an emerging technology to a foundational capability within modern enterprises. As AI systems become more deeply embedded in business operations, the need for clear, actionable and trustworthy risk-management practices has intensified. In response, a growing ecosystem of standards, regulations and frameworks is helping organisations structure how they identify, assess and govern AI-related risks.

	ISO/IEC 42001	EU ARTIFICIAL INTELLIGENCE ACT	NIST AI RISK MANAGEMENT FRAMEWORK
	VOLUNTARY STANDARD	REGULATION	VOLUNTARY FRAMEWORK
TYPE	Globally applicable	Providers and deployers of AI systems in the EU	Use-case agnostic
FOCUS	AI management system	Risk-based requirements	AI risk management

Three of the most influential approaches are ISO/IEC 42001, the EU Artificial Intelligence Act, and the NIST AI Risk Management Framework (AI RMF). ISO/IEC 42001 provides a voluntary, globally applicable management-system standard specifically designed for AI. Much like ISO 27001 for cyber security, it offers organisations a systematic governance structure to ensure responsible, transparent and controlled use of AI technologies. The EU AI Act, by contrast, represents a binding regulatory regime. It introduces risk-based obligations for providers, developers and deployers of AI systems placed on the European market, with significant emphasis on transparency, data governance, human oversight and accountability.

The NIST AI RMF complements these by offering a flexible, non-regulatory framework suitable for organisations worldwide. It focuses on fostering trustworthy AI through structured risk identification, measurement and mitigation. Importantly, NIST's approach is use-case agnostic, making it practical for varied sectors and maturity levels.

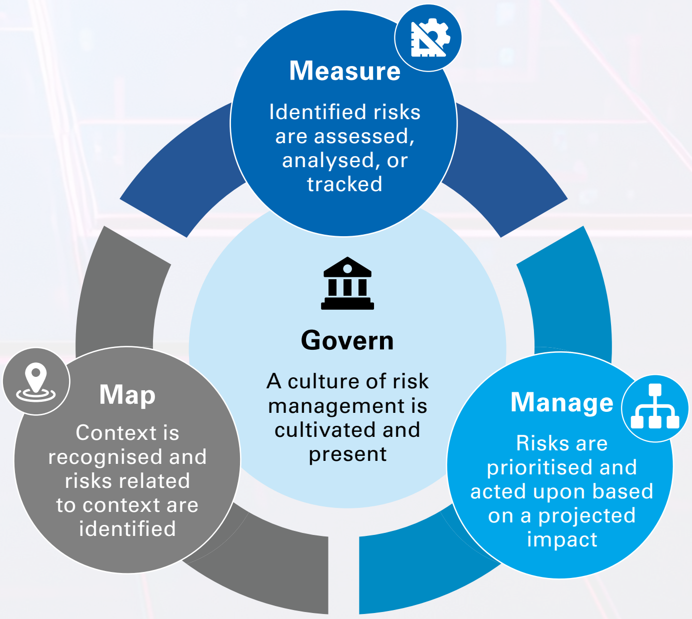
Together, these instruments demonstrate that organisations are not starting from scratch: a substantial body of guidance now exists to help enterprises manage AI risks effectively. For a global insurer like TMHCC, understanding and aligning with these frameworks supports stronger governance, informed decision-making and more resilient client partnerships.

Deep dive: NIST AI RMF

The NIST AI RMF is designed to help individuals, organisations and society develop and implement trustworthy AI applications. Developed through an extensive, multistakeholder process, the framework provides a structured yet adaptable method for governing AI-related risks across the full lifecycle of systems – design, development, deployment, monitoring and eventual retirement.

At its core, the AI RMF encourages organisations to embed risk management into everyday decision-making. While the framework is organised around four key functions – Govern, Map, Measure and Manage – NIST intentionally avoids prescribing rigid requirements. Instead, the AI RMF offers principles and outcomes that organisations can interpret and tailor to their own risk appetite, regulatory context and operational complexity. This makes the framework particularly valuable for global enterprises such as TMHCC, which must accommodate differing legal regimes and business models across regions.

AI Risk Management Framework


Measure
Identified risks are assessed, analysed, or tracked
Govern
A culture of risk management is cultivated and present
Map
Context is recognised and risks related to context are identified
Manage
Risks are prioritised and acted upon based on a projected impact

Source: National Institute of Standards and Technology. **AI Risk Management Framework** (January 2023)

NIST AI RMF: Profiles

Another important component is the concept of AI RMF Profiles. Profiles allow organisations to tailor the framework to specific use cases or sectors by selecting relevant outcomes from the RMF and adapting them to the context in which an AI system operates. A profile can be high-level (e.g., organisation-wide AI governance) or narrowly focused (e.g., a specific underwriting model or customer-facing decision tool). By using profiles, organisations can demonstrate alignment with the RMF in a structured, repeatable and evidence-based manner – useful not only for internal governance but also for external stakeholders, regulators and business partners.

NIST AI RMF: Playbook

A distinctive feature of the AI RMF is its companion resource, the NIST AI RMF Playbook. The Playbook translates the framework’s high-level concepts into actionable guidance by providing suggested activities, references and implementation considerations. These elements are not mandatory checklists but flexible tools that help organisations identify practical steps appropriate to their environment. For example, the Playbook outlines approaches for risk identification, documentation, validation and ongoing monitoring, all designed to make responsible AI governance operational rather than purely conceptual.

Overall, the NIST AI RMF and its supporting resources provide clear, practical scaffolding for building AI risk management capabilities that scale as organisational maturity grows. Their flexibility supports consistent application across diverse AI portfolios, helping firms balance innovation with robust oversight.

Conclusion

AI continues to reshape the risk landscape, introducing both opportunities and new complexities for businesses worldwide. For insurers such as TMHCC, effective AI risk governance is essential in understanding and underwriting emerging exposures faced by clients, as well as managing internal use of AI. Embedding frameworks such as NIST AI RMF, ISO/IEC 42001, and the EU AI Act into existing enterprise risk and governance structures strengthens organisational resilience and supports responsible, sustainable innovation. As AI evolves, maintaining disciplined, forward-looking risk-management practices will be critical to ensuring trust, transparency, and long-term business value.

Bibliography:

Source: European Parliament. **EU AI Act: first regulation on artificial intelligence** (June 2023)
https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

Source: Future of Life Institute. **The EU Artificial Intelligence Act** (December 2025)
https://artificialintelligenceact.eu/

Source: European Data Protection Supervisor. **Guidance for Risk Management of Artificial Intelligence systems** (November 2025)
https://www.edps.europa.eu/system/files/2025-11/2025-11-11_ai_risks_management_guidance_en.pdf

Source: International Organization for Standardization. **ISO/IEC 42001:2023 Information technology — Artificial intelligence — Management system** (2023)
https://www.iso.org/standard/42001

Source: International Organization for Standardization. **ISO 31000:2018 Risk Management — Guidelines** (2018)
https://www.iso.org/standard/65694.html

Source: National Institute of Standards and Technology. **AI Risk Management Framework** (January 2023)
https://airc.nist.gov/airmf-resources/airmf/

Source: National Institute of Standards and Technology. **NIST AI RMF Playbook** (March 2023)
https://airc.nist.gov/airmf-resources/playbook/

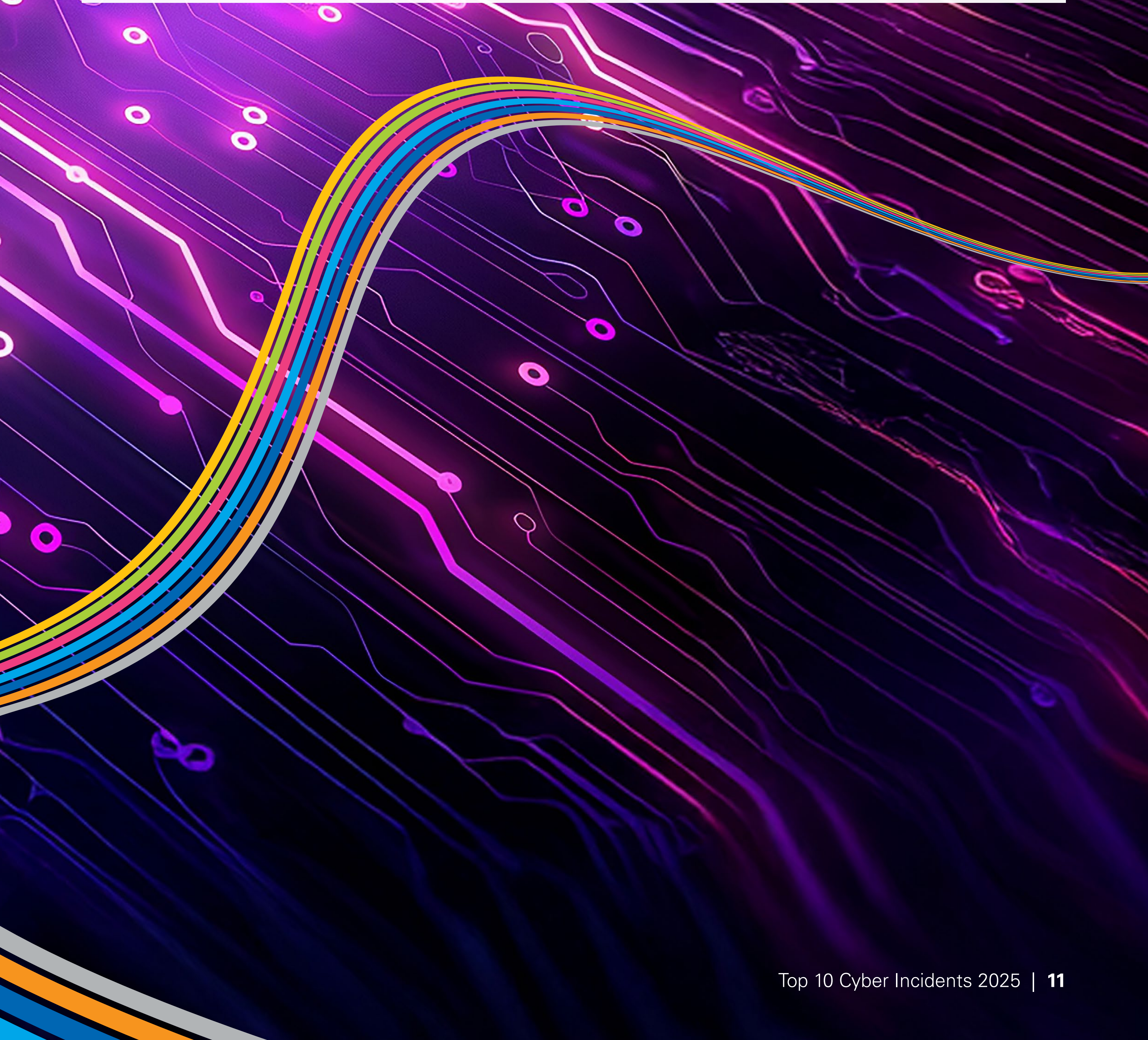
Cyber at Tokio Marine HCC

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
The St Botolph Building,
138 Houndsditch,
London, EC3A 7BT
Tel: +44 (0)20 7648 1300

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

Senior 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, which is a member of the Tokio Marine HCC Group of Companies. HCC International Insurance Company plc is authorised by the Prudential Regulation Authority (PRA) and regulated by the UK Financial Conduct Authority (FCA) and Prudential Regulation Authority. Registered in England and Wales No. 01575839 with registered office at The St Botolph Building, 138 Houndsditch, London, EC3A 7BT.

Information detailed within this marketing material is for promotional use only and does not constitute advice or fact. Any reliance upon such information shall be at your sole risk.