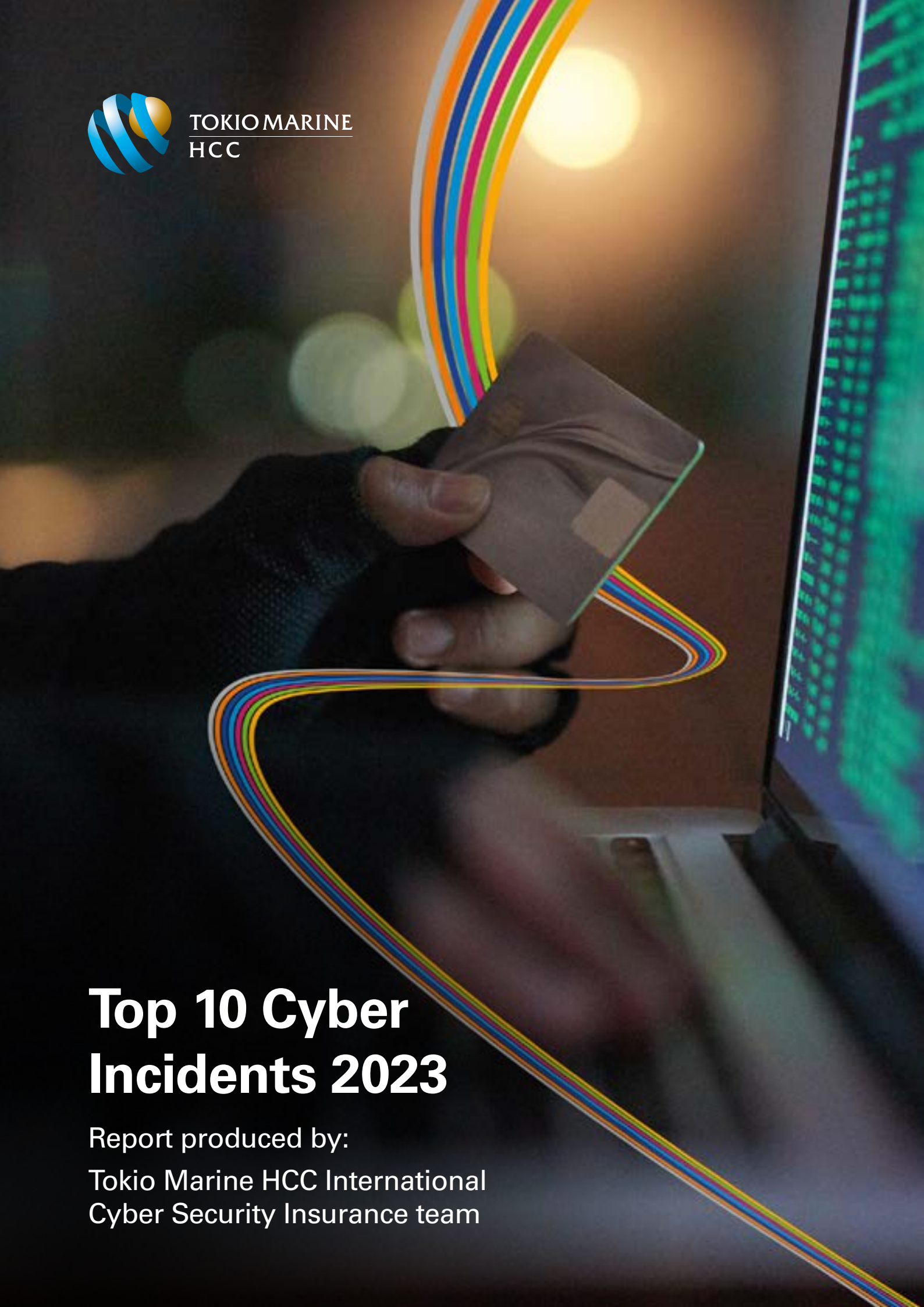

TOKIO MARINE HCC

Top 10 Cyber Incidents 2023

Report produced by:

Tokio Marine HCC International Cyber Security Insurance team

Top 10 Incidents 2023

2023 will be remembered for the continued increase of ransomware attacks, in severity and number. After a relatively calm first quarter of 2022, ransomware attacks made a comeback in the last two quarters of that year and exponentially increased throughout 2023. A prime example of this is the new LockBit criminal orgnisation – back in action and impacting scores of leading companies worldwide, across all sectors.

Unfortunately, Nation State attacks have also continued in 2023 due to Russia's persistent invasion of Ukraine and the armed conflict between Israel and Hamas-led Palestinian militant groups in Gaza. This has demonstrated that cyber-attacks are an important element in modern warfare.

Finally, in terms of the regulatory framework, 2022 introduced many new IT or cyber-related regulations: most notably, DORA (EU Digital Operational Resilience Act) and CIRCIA (U.S. Cyber Incident Reporting for Critical Infrastructure Act). However, 2023 has overtaken the previous year with the introduction of two considerable changes, which will need to be carefully monitored and implemented over the following months: New SEC (U.S. Securities and Exchange Commission) rules regarding Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure by Public Companies; and the new AI Act (EU Artificial Intelligence Act).

In this report, Isaac Guasch and Marc Pujol, our in-house cyber security specialists, have compiled a list of the worst and most significant cyber incidents from 2023 in terms of financial impact and reputational damage.

This year's "Bonus Track" focuses on artificial intelligence (AI), its evolution and diversification – undoubtedly one of the most fascinating and controversial talking points in 2023 and the years to come. Finally, we also look at the enormous potential that applications of generative AI have for cyber security professionals.

1 Israel - Hamas war

(Nation State attack)

SOURCE

Impact

Kinetic cyber attack causing direct or indirect physical damage, injury or death to people.

On 7 October, Hamas-led Palestinian militant groups conducted surprise-attacks in southern and central Israel, killing numerous civilians. According to Cloudfare, a few minutes after the military operation started, a large DDoS attack was detected against websites that provided critical information and alerts to civilians on rocket attacks.

In addition to the DDoS attacks, the criminal group AnonGhost also exploited a vulnerability in a mobile app that alerts Israeli civilians. Among other exploitations, the criminals could intercept requests and send fake alerts to app users.

ION Derivatives

2

(Financial institution)

SOURCE

Impact

Systemic risk due to supply chain attack causing large-scale business interruption.

On 31 January, ION Cleared Derivatives, a division of ION Markets (a widely used trading, funding, asset and risk management solutions provider within the financial sector), reported experiencing a cybersecurity event that affected some of their services.

The attack not only caused business interruption at ION but also at some of the world's largest banks, disrupting millions of clients' operations as a knock-on effect. The disruption impacted regulators too, as the Commodity Futures Trading Commission (the main US derivatives regulator) was unable to publish its weekly Commitments of Traders report; a report that shows the contracts that customers have been buying and selling.

MoveIT

3

(IT provider)

SOURCE

Impact

Systemic risk due to supply chain attack causing large-scale data breaches.

On 31 May, a new vulnerability was discovered in the MOVEit file transfer app by the software provider Progress. The vulnerability consisted in an SQL injection that could allow an unauthenticated attacker to gain access to MOVEit Transfer's database.

Depending on the database engine used (MySQL, Microsoft SQL Server, or Azure SQL), an attacker could infer information about the structure and contents of the database and execute SQL statements and, in doing so, alter or delete database elements.

MOVEit is used by thousands of organisations and their supply chains around the world. Therefore, numerous companies using or relying on the MOVEit app have suffered data breaches. For example, customer data was stolen from Ofcom, Transport for London, BBC, Boots and British Airways, amongst others.

ICBC

4

(Financial Institution)

SOURCE 1

SOURCE 2

Impact

Ransomware attack on one of the world's largest banks.

On 8 November, the US subsidiary of ICBC (Industrial and Commercial Bank of China) – the world's largest lender by assets – fell victim to a ransomware attack that interrupted some of their systems, including those used to clear US treasury trades and repo financing. This resulted in a temporary delay in its payments to counterparties.

The attack was claimed by the LockBit 3.0 cybercrime group on their official dark web site, with the LockBit representative saying: "They paid a ransom, deal closed". However, the Chinese foreign ministry spokesperson Wang Wenbin did not confirm this, but only stated in a regular press conference: "ICBC is closely following this and has taken effective emergency response measures and engaged in proper supervision and communication in order to minimise risk, impact and damage."

Caesars and MGM Casinos 5

(Gambling)

SOURCE 1 SOURCE 3
SOURCE 2 SOURCE 4

Impact

Ransomware attack with data breach on two of the largest casinos in Las Vegas.

On 7 September, Caesars Entertainment, Inc. reported to the U.S. Securities and Exchanges Commission (SEC) that the company "recently identified suspicious activity in its information technology network resulting from a social engineering attack on an outsourced IT support vendor used by the Company." Non-official sources confirmed that a 15M USD ransom was paid.

On 5 October, MGM Resorts International confirmed they had also been hit by an attack. The official press release stated that the company had identified a cybersecurity issue affecting a number of their systems and that investigation into the issue was ongoing. "On or around September 29, 2023, we determined that an unauthorised third party obtained personal information of some of our customers on September 11, 2023." MGM representatives confirmed the attack had an estimated impact of 100M USD.

Both attacks have been attributed to the same cybercriminal group – "Scattered Spider" or "Roasted 0ktapus," an affiliate of the Blackcat ransomware group.

Marina Bay Sands 6

(Hospitality & Accommodation)

SOURCE

Impact

Data breach of 665,000 customers' personal information.

On 7 November, Marina Bay Sands published a press release confirming that the company "became aware of a data security incident on 20 October 2023 involving unauthorised third-party access on 19 and 20 October 2023 to some of our customers' loyalty programme membership data."

An initial investigation determined that an unknown third party accessed the customer data – including personal data such as name, email, mobile phone number, country of residence and membership information – of 665,000 non-casino reward programme members,.

So far, official sources have not mentioned any ransom demand but the potential worth of the stolen data on the dark web is significant considering the number of records and the information they contain.

Air Europa 7

(Transportation)

SOURCE 1
SOURCE 2

Impact

Data breach of payment information and credit cards, including CVV codes, and significant reputational damage.

On 29 September, Air Europa detected a cyber-attack that compromised credit card data during payment processing. The incident occurred intermittently between 22 August and 29 September, posing a threat to data in transit and leading to the exfiltration of information related to customer credit cards, including card numbers, expiration dates and CVV codes.

Although there is no official confirmation about the number of clients impacted, the compromised data may be worth millions on the dark web. AirEuropa may also face a fine imposed by regulators, as they did back in 2018, when they were fined 600,000 EUR by the Spanish data protection authorities (AEPD) due to another data breach.

While the incident occurred in the payment environment of their web transactions, Air Europa reported no evidence of the leaked data being used for fraudulent activities. Despite the situation being under control, Air Europa notified affected individuals via email, strongly recommending the cancellation of compromised cards to prevent unauthorised charges or fraud.

UK Royal Mail 8

(Postal Services - Critical National Infrastructure)

SOURCE

Impact

Ransomware attack causing service disruption and reputational damage. Initial ransom demand of 80M USD.

On 6 February, the Russia-linked LockBit criminal organisation listed the Royal Mail Group on the victims list of their official dark web site. Royal Mail is deemed a critical national infrastructure to the UK. The cyber-attack affected its IT system, forcing the company to halt its international shipping services due to severe service disruption.

A ransom was set at 80 USD million, but Royal Mail refused to pay. Shortly after, the negotiation history was leaked by the LockBit group on their site on the dark web, untapping that negotiations lasted nearly a month, due to Royal Mail's negotiation skills, "bamboozling" and "stalling techniques".

Boeing 9

(Aircraft Manufacturing)

SOURCE

Impact

Ransomware attack causing more than 43GB of data leaked.

On 27 October, Boeing appeared on the victims list of the official dark web site of the Russia-linked LockBit criminal group. The attackers allegedly breached the company's systems via a zero-day exploit and were able to deploy the LockBit 3.0 ransomware to exfiltrate sensitive data.

Two weeks later, on 10 November, after Boeing refused to pay the ransom, LockBit released more than 43GB of exfiltrated data on their site. Among the files were configuration backups for IT management software and logs for monitoring and auditing tools.

Largest DDoS attack 10

(IT infrastructure providers)

SOURCE 1

SOURCE 2

Impact

Largest DDoS attack targeting major infrastructure providers.

In August 2023, Google's global load-balancing and DDoS mitigation infrastructure stopped the largest DDoS attack to-date: a two-minute attack that peaked at 398 million requests per second (rps), more than seven times larger than last year's largest-recorded DDoS attack.

Google stated that their investigation revealed the use of a novel "Rapid Reset" technique in the attack, which leverages stream multiplexing, an HTTP/2 protocol feature, and has affected many online infrastructure companies.

DDoS attacks can have wide-ranging impacts to victim organisations, including loss of business and unavailability of mission critical applications, which often cost victims time and money.

Bonus Track

1 Highlights of Artificial Intelligence in 2023

Whereas 2022 will be known as the beginning of a massive public integration of generative Artificial Intelligence (AI) – thanks in large to the release of ChatGPT and as already covered in our 2022 Top 10 Cyber Incident Report – 2023 will be known for the rapid evolution and diversification of AI.

In this context, exciting new generative AI has emerged this year, indicating a crucial time in the development of this transformative technology. The most well-known models to date include:

- ChatGPT (OpenAI)
- DALL-E (OpenAI)
- Midjourney (Midjourney, Inc)
- Stable Diffusion (Stability AI)
- Bard (Google)
- Gemini (Google)
- Bing chat / Copilot (Microsoft)
- Claude (Anthropic)
- LlaMA (Facebook)
- Grok (X / Former Twitter)
- Amazon Q (Amazon).

Since ChatGPT became available to the public, the AI landscape has witnessed a cascade of advances, breakthroughs and innovation. This timeline encapsulates the most notable highlights and milestones that have shaped AI and generative AI during 2023.

30 Nov 2022
OpenAI introduces **ChatGPT** to the world.

24 Feb 2023
Facebook releases **LLaMA**, a foundational, 65-billion-parameter large language model.

14 Mar 2023
OpenAI releases **GPT-4** and Anthropic releases **Claude**.

21 Mar 2023
Google releases **Bard**.

4 May 2023
Microsoft releases Bing chat (now **Copilot**).

2022 | 2023

NOV | JAN | FEB | MAR | APR | MAY | JUN

23 Jan 2023
After its 1bn USD investment in July 2019, **Microsoft extends its long-term partnership with Open AI** with a 10bn USD investment. Microsoft presents the **Azure OpenAI service** that includes several AI models made by OpenAI, including ChatGPT, Codex and DALL-E.

22 Mar 2023
Open letter asking to 'pause' AI development for six months due to ethical concerns, by thousands of technologists, incl. Elon Musk and Steve Wozniak.

23 Mar 2023
OpenAI introduces **AI plugins in ChatGPT**, designed specifically for language models with safety as a core principle, helping ChatGPT access up-to-date information, run computations, or use third-party services.

28 Mar 2023
Microsoft announces **Security Copilot**, a system that leverages GPT4 generative AI model to empower security professionals to defend their organisations.

6 Jul 2023
OpenAI announces code interpreter plugin (**Advanced Data Analysis**), allowing ChatGPT to run code (with access to uploaded files), to analyse data, create charts, edit files, perform math, etc.

20 Jul 2023
OpenAI announces **custom instructions**, giving users more control over ChatGPT's responses.

25 Sep 2023
OpenAI rolls out new voice and image capabilities to give **ChatGPT** the ability to 'see', 'hear' and 'speak'.

4 Nov 2023
xAI announces **Grok** – model with real-time knowledge of the world via X (former Twitter) – finally rolled out 7 Dec.

6 Nov 2023
OpenAI introduces **GPTs**, able to create custom versions of ChatGPT that combine instructions, extra knowledge, and any combination of skills.

6 Dec 2023
Google announces **Gemini**, a multimodal generative AI model that combines different types of information incl. text, code, audio, image and video.

2023

JUL | **AUG** | **SEP** | **OCT** | **NOV** | **DEC**

28 Aug 2023
OpenAI launches **ChatGPT Enterprise**, offering enterprise-grade security and privacy, unlimited higher-speed GPT-4 access, longer context windows for processing longer inputs, advanced data analysis capabilities, customisation options, etc.

30 Oct 2023
U.S. president Biden's Administration releases **E.O. 14110** on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence – the first regulation of its kind to be approved.

17 Nov 2023
Sam Altman, CEO of **Open AI**, is removed by the board, but returns shortly after, as employees threaten to quit – testimony to power play in the AI insdustry.

28 Nov 2023
AWS announces **Amazon Q**, a generative AI-powered assistant designed for work.

8 Dec 2023
European Parliament and Council negotiators reach a provisional agreement on the **EU AI Act**.

2 Artificial intelligence meets cybersecurity

In the ever-evolving landscape of cybersecurity, security professionals face an ongoing challenge against relentless and sophisticated attackers. This, coupled with a global shortage of skilled security professionals, creates a challenging scenario for organisations worldwide. As the frequency and intensity of cyber threats continue to rise, the need for innovative solutions becomes imperative.

Artificial intelligence (AI) and particularly, generative AI, can play a key role in cybersecurity. By leveraging models like OpenAI's GPT-4, new innovative cybersecurity solutions are being released.

Microsoft Security Copilot is one such solution amongst others currently being released. It aims to empower security professionals by combining advanced large language models (LLM), security-specific skills and global threat intelligence in order to enhance incident detection, response speed and overall security stance. The system simplifies complexity, accelerates responses and continually learns, enhancing security teams' capabilities. By summarising threat intelligence and correlating data, MS Security Copilot aids in identifying and prioritising threats, bridging any knowledge gaps, and addressing any skill shortages in cybersecurity. It provides end-to-end defence at machine speed.

In addition, MS Security Copilot continually learns from user interactions and adjusts its responses to provide more coherent, relevant and useful answers over time. This adaptive learning approach ensures a constant improvement in the system's capabilities.

In the world of cybersecurity, where every minute counts, tools like MS Security Copilot are becoming crucial. Their ability to surface prioritised threats in real-time and anticipate threat actors' moves based on continuous reasoning sets a new standard for security AI capabilities.

Although AI was widely used in cybersecurity tools as part of their "Big Data" capabilities, the arrival of generative AI opens a new world of possibilities. Tools like MS Security Copilot that leverage generative AI to enhance the collaboration of AI and professionals, are establishing a new standard for the industry.

AI bibliography:

https://openai.com/blog/chatgpt
https://news.microsoft.com/2019/07/22/openai-forms-exclusive-computing-partnership-with-microsoft-to-build-new-azure-ai-supercomputing-technologies/
https://blogs.microsoft.com/blog/2023/01/23/microsoftandopenaiextendpartnership/
https://openai.com/blog/chatgpt
https://www.anthropic.com/index/introducing-claude
https://blog.google/technology/ai/bard-google-ai-search-updates/
https://www.reuters.com/technology/google-begins-opening-access-its-chatgpt-competitor-bard-2023-03-21/
https://futureoflife.org/open-letter/pause-giant-ai-experiments/
https://openai.com/blog/chatgpt-plugins
https://blogs.microsoft.com/blog/2023/03/28/introducing-microsoft-security-copilot-empowering-defenders-at-the-speed-of-ai/
https://blogs.microsoft.com/blog/2023/05/04/announcing-the-next-wave-of-ai-innovation-with-microsoft-bing-and-edge/
https://openai.com/blog/chatgpt-plugins#code-interpreter
https://openai.com/blog/custom-instructions-for-chatgpt
https://openai.com/blog/introducing-chatgpt-enterprise
https://openai.com/blog/chatgpt-can-now-see-hear-and-speak
https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/
https://x.ai/
https://openai.com/blog/introducing-gpts
https://aws.amazon.com/about-aws/whats-new/2023/11/aws-amazon-q-preview/
https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai
https://www.euaiact.com/
https://news.microsoft.com/2023/03/28/with-security-copilot-microsoft-brings-the-power-of-ai-to-cyberdefense/
https://blogs.microsoft.com/blog/2023/03/28/introducing-microsoft-security-copilot-empowering-defenders-at-the-speed-of-ai/
https://blog.google/technology/ai/google-gemini-ai/
https://www.microsoft.com/es-es/security/business/ai-machine-learning/microsoft-security-copilot

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