

2024 cybersecurity regional trends

Global strategies, local tactics



Digital Security Magazine

2024 cybersecurity regional trends

01
France

02
DACH region

03
UK and Ireland

04
MEA

05
APAC

06
North America

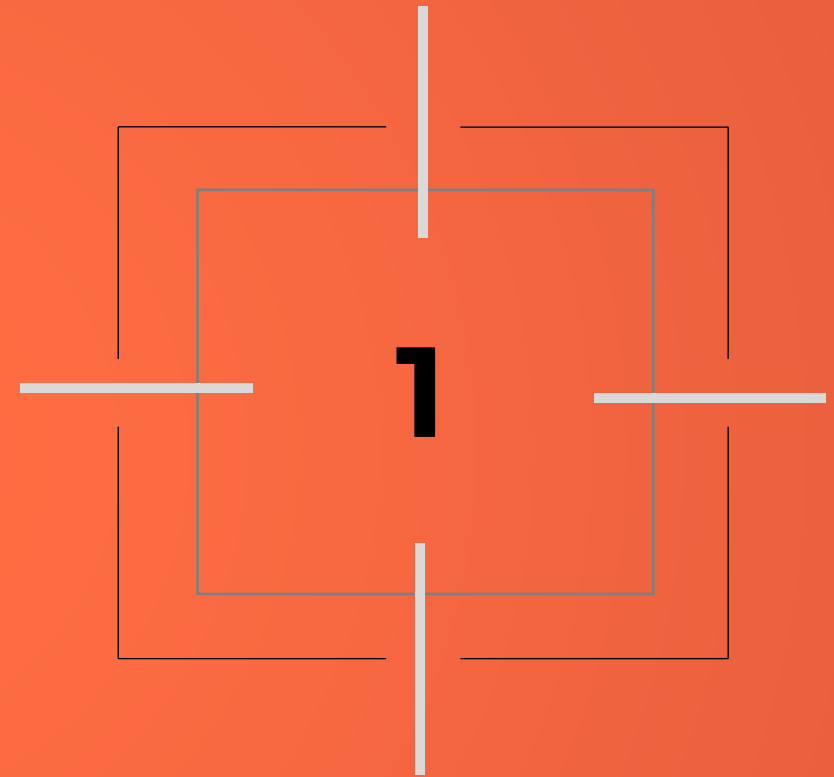
EVIDEN

France

Insights from Jean-Baptiste Voron

Chief Technical Officer

Eviden Cybersecurity France



What local regulations are expected to come into action in France in 2024?

In France, the regulatory landscape is very dense. In 2024, in addition to the NIS2 Directive, incorporating the Cyber Resilience Act and the IA Act into national law will be important. The evolution of ANSSI's roadmap on post-quantum risks should also trigger several inventory and compliance work. Finally, a few specific sectors are adopting their own regulations: in the healthcare sector, the ANS and CNIL are planning to reinforce the use of health data, while the public sector is prioritizing the use of secure (qualified) cloud services.

What technology, with different maturity, would you flag?

API Security: Niche state

Compared to protection of traditional flows based on infrastructure defense in depth, we can consider that API security is neglected. Indeed, current defense systems are not adapted to the threats specific to these technologies. Yet the API revolution is well underway. Behavioral analysis and detection of weak signals are the keys to the protection strategy to be implemented.

Data Encryption: Partially adopted

Data encryption is part of an overall cybersecurity strategy. Methods and tools are numerous, from the simplest to the most complicated. Yet all too often, they remain unused due to lack of planning, skills, and investment. Yet this component is essential to address sovereignty issues, i.e. a European mainstream topic.

Threat Intelligence: Widespread use, though limited by skills gap

Threat Intelligence (TI) technologies are now widely adopted in France. But skills are still in short supply to make the full value of this content actionable. The TI platform and Security Orchestration, Automation and Response (SOAR) approaches are attempting to bridge this gap. The gradual adoption of Cloud environments and the rise of DevSecOps teams are accelerating this trend.

What are the major scopes of investments planned by the institutions, governments, public actors in France in 2024?

Compliance with European standards (and their local incorporation into national law) will undoubtedly form a large part of the projects and expenses of public-sector institutions in 2024. The adoption of the Cloud will be the other key trend of the coming year.

What cyber event or data breach that occurred in 2023 had a significant resonance or impact in France?

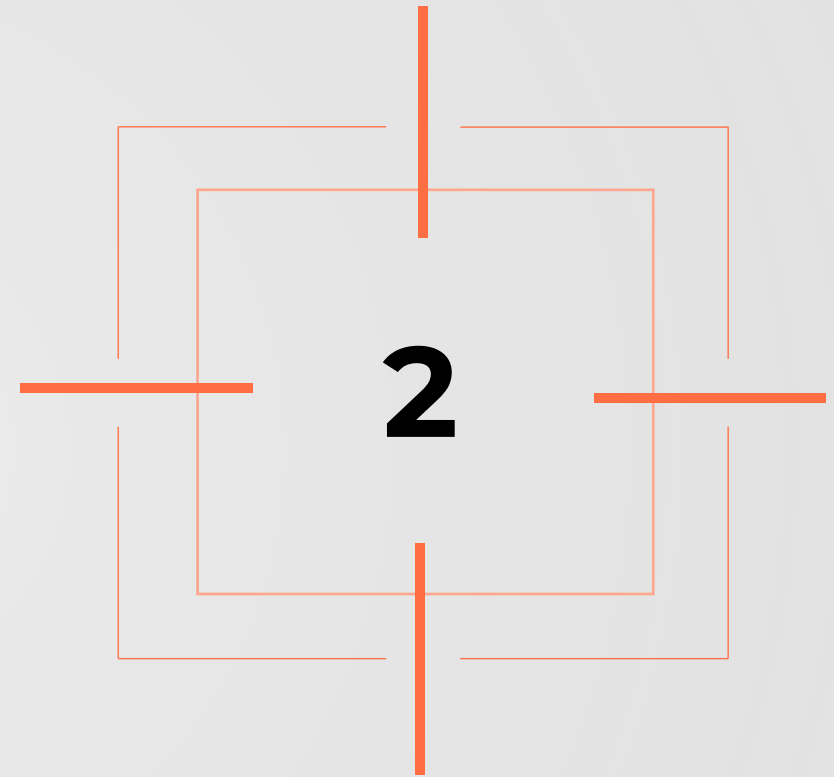
Cyber-attacks targeting hospitals and local authorities were particularly numerous in France in 2023. Most of them resulted in data leakage, leading all citizens to measure the dispersion and vulnerability of their personal data. In France, the priority is to reinforce cyber hygiene measures, rather than launching an innovative plan for GenAI Cyber.

DACH region

Insights from Daniel Noszian

Team lead SOC consulting

Cybersecurity DACH



What local regulations are expected to come into action in the DACH region in 2024?

Recently introduced EU-wide cybersecurity regulations such as NIS2, the Cyber Resilience Act (CRA), the Digital Operational Resilience Act (DORA), the Directive on the Resilience of Critical Entities or the EU Cloud Services Cybersecurity Scheme are expected to have a significant impact on both the public and private sectors in the Austrian region. Legislative and regulatory activity currently confirmed for 2024 is focused on the implementation and transposition of these regulations into national law, with the NIS2 Directive at the forefront.

In the landscape of evolving cybersecurity regulations, public and private sector entities in the DACH region are increasingly grappling with the complexities of the NIS2 directive. There is a pervasive sense of being overwhelmed due to a lack of clear information and guidance

on the scope, applicability, and extent of the directive, as well as the tangible outcomes expected from its implementation. This ambiguity may contribute to further misunderstandings and confusion about the full scope of NIS2: for example, companies that are not directly subject to NIS2 are nevertheless obliged to improve their security and compliance measures, as they may be integral parts of supply chains that indirectly affect critical infrastructure (c.f. NIS2's "all-hazards approach" to cybersecurity risk management). This challenge is compounded by the lack of concrete implementation guidance for a wide range of non-NIS2 frameworks that will come into force. This gap in clarity and direction creates an urgent need for more detailed and actionable guidance to effectively navigate the complex web of cybersecurity obligations.

What technology, with different maturity, would you flag?

OT Security: Niche state

While the need to protect OT environments (and related critical infrastructure implementations) has crossed a critical threshold of awareness, the actual deployment of dedicated OT security solutions or services is still lagging far behind. Basic measures (zoning, firewalling, segmentation) are being increasingly adopted, but proactive OT protection is still in its infancy.

Managed Detection and Response (MDR): Niche state

In the DACH region, this advanced Detection and Response technology is often misrepresented or mistaken with various related services like Managed Security, SOC-as-a-service or similar. There is also marketing fatigue among cybersecurity decision makers. Besides, vendors and service providers are failing to demonstrate differentiators and/or added value.

Endpoint Detection and Response (EDR): On-going widespread

This technology is undergoing widespread implementation.

Nevertheless, companies still lack resources and skills to leverage full EDR potential by tapping into hunting and preventive capabilities.

What are the major scopes of investments planned by the institutions, governments, public actors in the DACH region in 2024?

In 2024, the cybersecurity investment landscape is expected to be dominated by several key areas. Foremost among these is an enhanced focus on Cloud Security, driven by the need to navigate the complexities of cloud-based IT infrastructures.

Concurrently, there will be a strong emphasis on Vulnerability Management and Identity & Access Management, underscoring the critical importance of securing both logical and technical access layers, and identifying potential security gaps.

Additionally, AI-Driven Cyber Defense will gain prominence as companies seek advanced solutions to manage the increasing data volumes and complexity in cybersecurity.

The development of Security Operation Centers/Managed Security Services will continue to be a significant area of investment, though with nuanced approaches in their implementation relative to external, hybrid and emerging models (MDR gaining momentum in the DACH region).

Finally, business continuity will remain a top priority, emphasizing the need for robust strategies to quickly recover from cyber incidents and ensure operational resilience.

What cyber event or data breach that occurred in 2023 had a significant resonance or impact in the DACH region?

Austria saw a notable spike in cyberattacks targeting local organizations in 2023, with figures from recent surveys suggesting an increase in the range of 50-80%. Despite this increase, the country did not experience any major headline-grabbing data breaches.

However, smaller incidents did occur, such as a security breach at an online wine retailer that resulted in a limited exposure of customer data, and a leak of 20,000 user records from a subcontractor of Magenta/T-Systems.

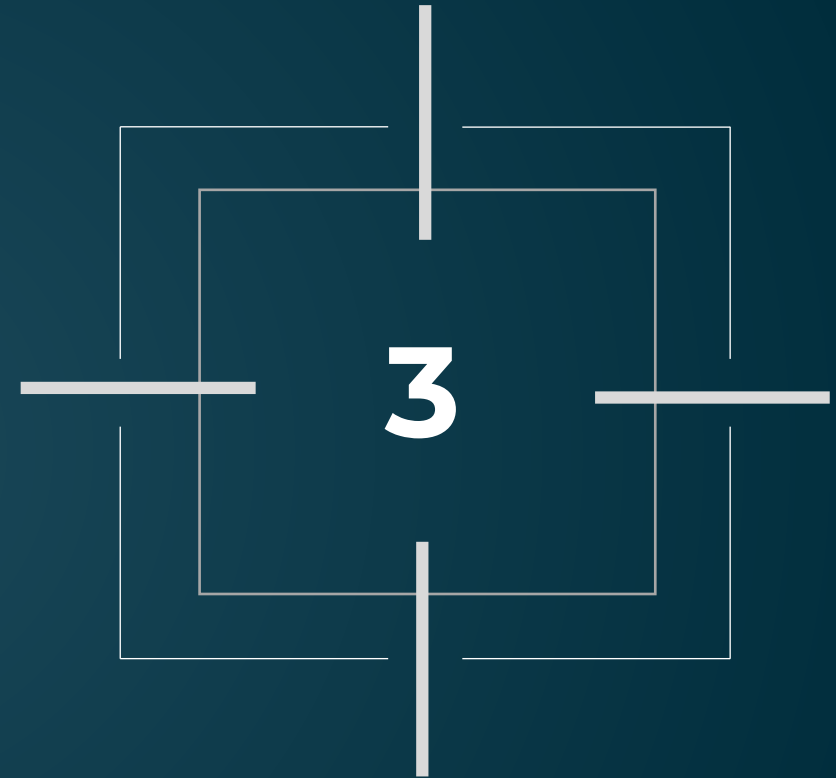
In the financial sector, the Move-it compromise earlier in the year had a limited impact. Evidence from Eviden SEC Defense's current project and investigation workload suggests a considerable number of unreported cases, a view supported by SEC Consult's ongoing research into the portrayal of cybercrime against Austrian companies on the dark web. To date, no significant policy changes or groundbreaking developments have emerged, but the significant increase in attempted cyberattacks has significantly influenced public discourse and catalyzed a strong push for enhanced cybersecurity measures by relevant authorities.

UK & Ireland

Insights from Terry Bebbington

UK Cloud and Advisory Lead

Eviden Northern Europe



What local regulations are expected to come into action in the UK and Ireland in 2024?

The Digital Operational Resilience Act (DORA) will have a significant impact on companies in the Financial Markets sector operating across the European Union.

What technology, with different maturity, would you flag?

Managed Detection and Response (MDR) – on-going widespread

MDR is a service offering typically wrapped around a set of technologies to deliver a set of outcomes, e.g. Advanced Detection and Response and Remediation against cyber-attacks. More clients are adopting or evolving their traditional SIEM technologies due to many factors – e.g. alert fatigue, inability to retain or hire a scarce set of specialized skills, and legacy cost and deployment models that struggle to scale with cloud adoption and migration strategies. More clients are looking to leverage third party specialist providers to either optimize and integrate innovative technologies into their detection and response ecosystems, and/or integrate a wide range of security and business applications, services, and platforms to scale with an ever-evolving digital estate. Due to the complexity and rapid rate of technological change in the detection and response paradigm most clients are struggling to keep up with the latest versions of MDR related technologies and platforms.

What technology, with different maturity, would you flag? *(continued)*

Endpoint Detection and Response (EDR) – Massively adopted

Most of our clients have some form of EDR platform or technology deployed across their digital estates. The main reason being it is seen as a foundational security technology building block in the mitigation of cyber threats targeting a client's endpoint estate. About 70-80% of successful cyber-attacks or breaches occur due to vulnerabilities exploited via the endpoint, hence the need to secure them and, as stated, EDR is one of the building blocks to mitigate this attack vector. The evolution of the EDR market now includes OT technologies but not all providers offerings are as mature as their traditional IT solutions. There are many EDR vendors in the market and evolving constantly, which requires clients to understand this market space.

CNAPP – Niche state

A recent advancement in the cloud security market is Cloud-Native Application Protection Platforms (CNAPP). CNAPP platforms provide a plethora of security features but fundamentally their core offerings are:

- Cloud Security Posture Management (CSPM);
- Cloud Service Network Security (CSNS);
- Cloud Workload Protection Platform (CWPP);
- Cloud Infrastructure Entitlements Management in a single holistic platform.

The value for clients offered by CNAPP is they aim to provide a single management pane of glass view of compliance, configuration monitoring and enforcement of cloud workload policy violations across the hybrid enterprise. We see this as a significant adoption technology for our clients struggling to meet their compliance mandates and addressing security gaps in their CI/CD pipelines.

What are the major scopes of investments planned by the institutions, governments, public actors in the UK and Ireland in 2024?

The UK Government has announced £18.9 million investment in Northern Ireland's Cyber Security industry, including £11 million Government funding through the New Deal for Northern Ireland, to develop a pipeline of cybersecurity professionals in NI as well as helping businesses and startups develop new opportunities

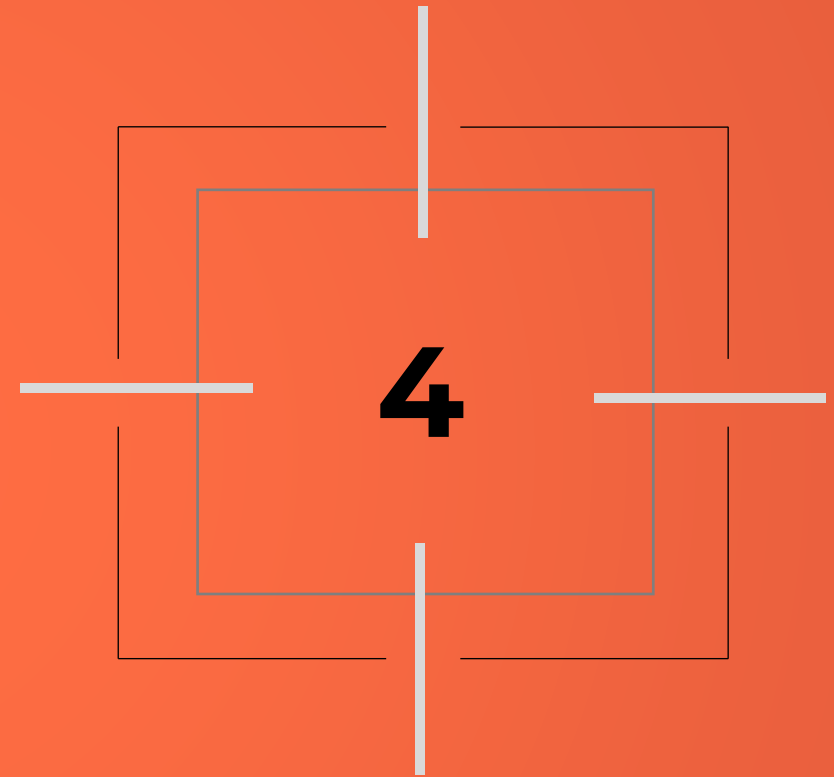
What cyber event or data breach that occurred in 2023 had a significant resonance or impact in the UK and Ireland?

Leak of personal information of all 10,000 serving police officers in Northern Ireland. This breach was described as "monumental" and "potentially calamitous" by the Police Federation of Northern Ireland, as it could expose the officers and their families to threats from dissident republicans and other criminals.

Middle East and Africa

Insights from Amit Roy
Head of Cybersecurity META

EVIDEN



What local regulations are expected to come into action in MEA in 2024?

MEA has seen a rapid increase in cybersecurity threats prompting governments of various countries in the region to come out with cybersecurity standards, such as Information Assurance Framework for UAE or the NCA (National Cybersecurity Authority) regulation, which would need public and private organizations to comply with.

Ensuring consumers' data privacy is also gaining paramount importance with new data privacy and protection legislations, within the region, driving consumer demands around trustworthy use of personal data. Privacy regulations such as PDPL (Personal Data Protection Laws) in Bahrain and Saudi Arabia, the Personal Data Privacy Protection Law in Qatar, the UAE Data protection Law, and the Personal Data Protection Law in Egypt, help protect the rights of the data subject with respect to lawful collection and use of their personal data by an organization and failing which could not only result in fines, reputational damage but also operational inefficiencies and loss of consumer trust.

What technology, with different maturity, would you flag?

OT security: Niche state

With the widespread of OT risks and the convergence of IT/OT/IOT, OT-security related investments are gradually increasing but still restricted to Oil/Gas and Utilities sector, and large enterprises.

Cloud Security: Partially adopted

With investments from hyperscalers (i.e. AWS, Google, Microsoft) more organizations are moving towards cloud, hybrid set up, and cloud security related controls would soon become widespread, while it's still in its early adoption stage.

Advance Detection and Response: On-going widespread

Gradual shift of organizations from a SIEM-as-a-service to MDR with the early adopters being more security-matured customers – like banks and large private companies. With the increase in more advanced cyber-attacks, next generation MDR/XDR players using AI/Gen AI would become more widespread.

Endpoint and Mobile security: Widely adopted and funded

The investments for new and refresh on endpoint-security related technologies and talents is quite mature in the MEA region with almost all technology vendors/partners investing in it.

What are the major scopes of investments planned by the institutions, governments, public actors in MEA in 2024?

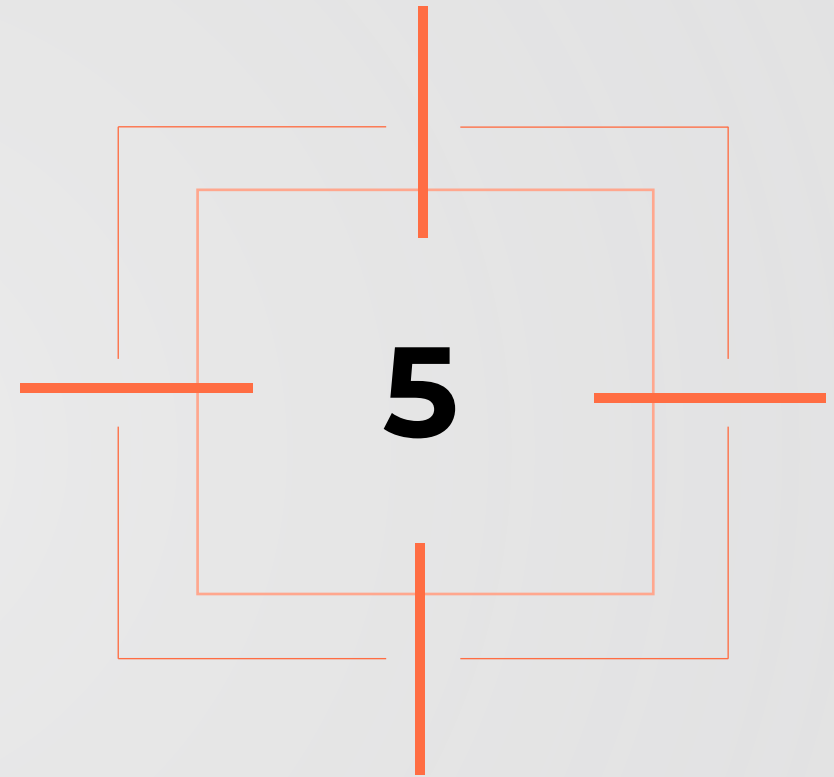
The region's transition to digitization has created an increase in cybercrime, prompting governments to strengthen the protection and integrity of their technological infrastructure by investing in newer cybersecurity regulation and data privacy laws. Large public and private enterprises are strengthening their threat detection and response capabilities by investing in AI to boost cybersecurity resilience. There is also renewed focus to improve data security in line with data sovereignty guidelines, while reaping the benefits of cloud adoption and adopting cloud security initiatives.

What cyber event or data breach that occurred in 2023 had a significant resonance or impact in MEA?

In the region, several of the cyber-attacks can be attributed to geopolitical risks including nation-state attacks. Several such attacks have taken place in the recent past including the likes of 'Anonymous Sudan' doing targeted DDOS attacks over Banks and Governments in the region. The region has also seen a wide increase of ransomware attacks by hacking groups across organizations. Such incidents have prompted organizations to invest in cyber defense strategies particularly in advance threat detection and response capabilities using AI and cyber resilience.

Asia Pacific

Insights from Chee Wooi Tan
Head of Big Data and Security APAC
and Jan de Meijer
Cybersecurity consultant



What local regulations are expected to come into action in the APAC region in 2024?

With Singapore as one of the main hubs of APAC, it will be interesting to follow the advisories of the Counter Ransomware Task Force (CRTF).

It is expected that various agencies will provide more detailed guidance on ransom payments, including the potential mandatory reporting of ransomware payments in Singapore.

What technology, with different maturity, would you flag?

To raise the general security posture of an organization, IAM and MDR/XDR technologies are some of the key technologies. They often are already adopted but require an increased maturity and holistic application.

What are the major scopes of investments planned by the institutions, governments, public actors in the APAC region in 2024?

There is a whole scale of technological developments that are the catalyst of the current transformations, and those are on the radar of organizations as potential investment opportunities. If we take a closer look at the similarities between those leading technologies and what is at its core, it can be observed that they always revolve around Artificial Intelligence, or GenAI. It is expected that an influx of investment funds will flow towards that.

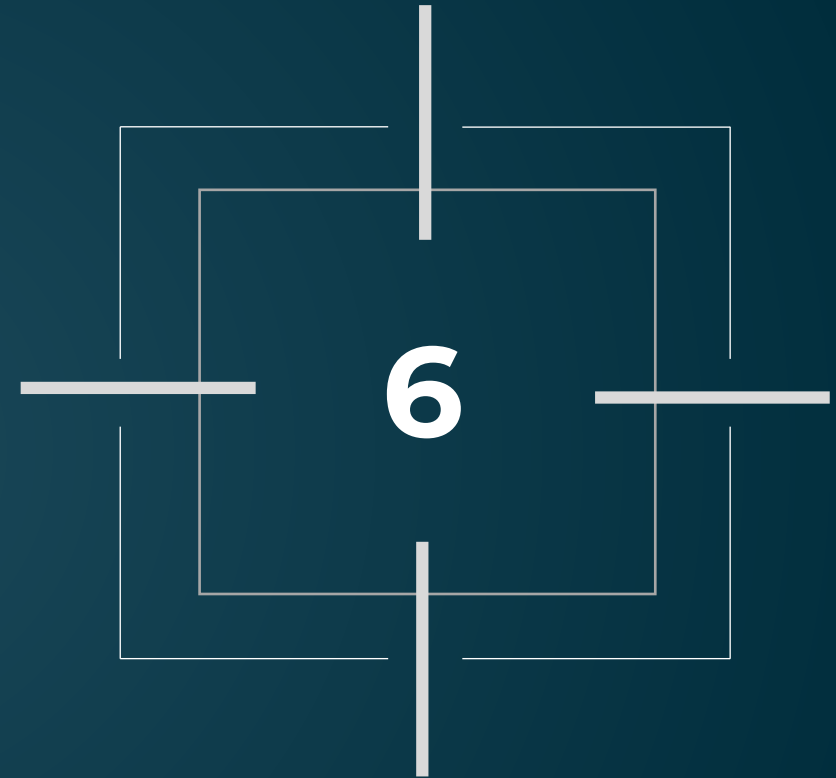
What cyber event or data breach that occurred in 2023 had a significant resonance or impact in the APAC region?

One notable ransomware attack and data breach is the [PhilHealth cyber-attack](#) in the Philippines, affecting the personal data of 13 million people. Consequently, the cyber awareness of organizations in the Philippines increased.

We observe a surge in inquiries on cyber expertise and/or services. This can be MDR, but it is also common that clients have no notion of where to start and simply turn to us for help and suggestions.

North America

Insights from Dean Weiner
Head of Cybersecurity Americas
and Sachin Varghese
Specialized Sales Manager



What local regulations are expected to come into action in North America in 2024?

- Undergoing crypto inventorying to comply with the [National Security Memorandum-10](#) which acknowledged the threat of quantum towards security and set a course of action to protect against it by migrating to post-quantum cryptography.
- In June 2023, and coming into action in 2024, the US SEC (Securities and Exchange Commission) adopted [Mandatory Cybersecurity Disclosure Rules](#) “that will require public companies to disclose both material cybersecurity incidents they experience and, on an annual basis, material information regarding their cybersecurity risk management, strategy, and governance.” ([SEC, 2023](#)) This enters into action for companies in 2024.
- State data privacy laws: Several states are considering or have enacted their own data privacy laws. These laws vary in their scope and requirements, but they could create a patchwork of data privacy regulations in the United States (update of the California Consumer Privacy Act ([CCPA](#)) on privacy policies, data privacy laws coming into effect in 2024 for Florida (FDBR), Texas (TDPSA), Oregon (OCPA), Montana (MTCDDPA), Delaware (DPDPA)).
- In [Canada](#), Consumer Privacy Protection Act and the accompanying Artificial Intelligence and Data Act.

What technology, with different maturity, would you flag?

Cyber Security Mesh Architecture (CSMA) – Partially adopted

CSMA is a new innovative approach to generate higher value from existing & new security investments through seamless integration & analytical use cases. Lack of common integration standards has been an area of key concern in the industry. CSMA breaks the silos with a common & deeper approach for integration. AWS has taken the lead with Open Cyber Security Framework (OCSF) that brings together a generic format for integrating security products.

Organizations in North America, frequently operating in a hybrid model with on-premises and cloud deployments, are more inclined towards adopting a distributed enterprise structure. This makes Security Mesh a more pertinent solution for these organizations.

Besides, Gartner has recognized CSMA as one of the top seven cybersecurity trends and predicts that organizations adopting mesh architecture will experience an average reduction of 90% in the financial impact of individual security incidents by 2024.

Artificial Intelligence (AI) – On-going widespread

The GAFAM are leading the widespread adoption of AI, including its latest iteration, GenAI, for various applications. In cybersecurity-specific use cases, AI is integrated into security technologies leading for example to cognitive detection and response.

According to a recent Gartner survey, 34% of organizations are already using or implementing AI application security tools to mitigate the risks associated with generative AI (GenAI).

However, further development and standardization of AI tools for security are still required.

What are the major scopes of investments planned by the institutions, governments, public actors in North America in 2024?

Ethical and secure use of AI

To safeguard the responsible and ethical development and application of artificial intelligence (AI), President Biden issued an [executive order](#) mandating AI transparency and accountability. This directive requires large AI developers and cloud providers to share safety testing data and insights with the U.S. government. Additionally, it instructs government agencies to set forth standards for safety and testing in the AI domain.

PQC – High investment forced by government.

The USA is ahead of the quantum disruption to security by obliging companies to perform a detailed cryptographic inventory of all asymmetric algorithms in use. Alongside the governmental actions, the National Institute of Standards and Technology (NIST) has initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. The winners of the competition will be disclosed in 2024 and lead to major transformation and investments for all enterprises worldwide.

What cyber event or data breach that occurred in 2023 had a significant resonance or impact in North America ?

The video game industry has been highly targeted by non-professional and/or young hackers. Early as in February 2023, Activision acknowledged the Call of Duty video game leak. It had significant resonance among the business as it originated from a simple theft of the login credentials of an HR employee via text message phishing, and it resulted in a major imagery leak prior to the « Modern Warfare III » opus release. Besides, later in the year, the GTA 6 leak forced the publisher Rockstar to spend \$5 million to recover damages. The leak was performed by an 18-year-old hacker from a hotel room.


The healthcare industry remains a classical target for hackers, as even if the ransom is not paid, the stolen data can easily be sold on the dark net. On December 11, 2023, Norton Healthcare suffered a data breach impacting an estimated 2.5 million people. The attacker gained unauthorized access to personal information not only about millions of patients but also employees.

Attackers do not spare public organizations who handle healthcare information either. Indeed, last September, Ontario's birth registry suffered a data breach of its systems, and around 3.4 million people who sought pregnancy care over the last decade have had their information accessed. It is estimated that 2 million babies born during this period have had their healthcare data exposed. This attack was a massive exploit of the now well-known vulnerability in the MOVEit file transfer tool.

EVIDEN

Thank you

Explore all our experts' 2024
cybersecurity predictions:

 [Eviden digital security magazine](#)

