Security Operations Center

STATE OF
CYBER SECURITY
2026

sopra steria

STATE OF CYBER SECURITY 2026

sopra steria

CONTENTS

EXECUTIVE SUMMARY

Nordic Threat Landscape: A Region Under Pressure

The Nordic region faces an intensifying mix of cybercrime, state-aligned operations, and hybrid campaigns that blend cyberattacks, sabotage, and disinformation. Its strategic position near Russia and NATO's northern flank makes it a prime target. Cybersecurity is now deeply tied to geopolitical risk, and the Nordics must prioritise strengthening the region's resilience and robustness across critical infrastructure and digital ecosystems.

Resilience: The Backbone of National Security

Critical infrastructure depends on digital systems, making resilience a strategic necessity. Modernisation and automation expand the attack surface, while geopolitical tensions heighten risk. Cyber incidents targeting essential services are rising, and continuity under pressure is paramount. Resilience requires embedded security, strong IT hygiene, and defendable operations to ensure that critical functions withstand prolonged disruptive attacks. In today's threat landscape, digital resilience is not optional; it is the foundation of national security and operational continuity.

Cloud Strategy Is Now a Question of National Resilience

Cloud is no longer just a business choice, it's a geopolitical risk. Control of digital infrastructure has shifted to global powers, making cloud decisions subject to sanctions, sovereignty mandates, and trade restrictions. Vendor lock-in amplifies exposure, reducing flexibility and resilience. Organisations must design for portability and multi-cloud strategies to maintain compliance, independence, and continuity in an unpredictable global landscape.

Facing the Most Transformative Technological Shift in Decades

Generative AI delivers unprecedented opportunities, but also expands the attack surface. Multimodal capabilities, endpoint integration, and rapid adoption create complexity that threat actors exploit for social engineering, automated attacks, and AI-driven post-exploitation. Organisations must implement AI-specific governance, secure development practices, and robust safeguards. Security strategies must evolve as fast as innovation, or risk severe compromise.

Attackers Don't Break In – They Log In

Identity remains the most common entry point for compromise, and fixing these basics is essential for maintaining security, and meeting regulatory requirements. Credential harvesting has become the primary objective for cyberattacks. Adversaries gain access through phishing, ClickFix, and other identity-focused techniques, allowing them to blend into normal activity and bypass traditional defenses. This shift makes identity-first security critical: enforce phishing-resistant MFA, least privilege access, and continuous monitoring to stop attacks before they spread.

Cyber Risk Has Your Name on It

Regulations like the Digital Security Act and DORA make cybersecurity a leadership responsibility. Boards and executives can now face personal liability and significant fines for serious breaches. Security can no longer be delegated, it must be embedded in governance, with clear accountability, documented risk management, and oversight of third-party dependencies. For you as a leader, this is not something you can choose to do; it's a legal and strategic imperative.

> "In today's threat landscape, digital resilience is not optional; it is the foundation of national security and operational continuity.

Outlook 2026: The Age of AI

In 2026, AI will accelerate both attacks and defences – fuelling malware development, deepfake-driven social engineering, and automated exploitation, while enabling faster detection and response. Identity compromise and supply chain attacks remain top risks, as state-backed campaigns target critical infrastructure and exploit trust links across cloud and on-prem environments. At the same time, regulations like NIS2 and DORA demand verifiable resilience and accountability. Survival requires Zero Trust, phishing-resistant MFA, least privilege access, and continuous verification – paired with strong IT hygiene and proactive risk governance.

A personal note

I hope you find this report informative and inspiring. As always at Sopra Steria we aim to share our insights, advice and experience regarding Cybersecurity in an informative way rather than publishing scary and dark reports that leave little room for hope. My wish is that you use this report to strengthen your work on your own Cybersecurity strategy, and that it helps you prioritise where to put extra effort in the coming year. I also hope that it gives you greater insights into what you should be discussing with your fellow management and security departments.

Best regards,

Jørgen Rørvik
Director of Cybersecurity
Sopra Steria Scandinavia
e-mail: Jorgen.rorvik@soprasteria.com

HOW TO NAVIGATE THIS REPORT

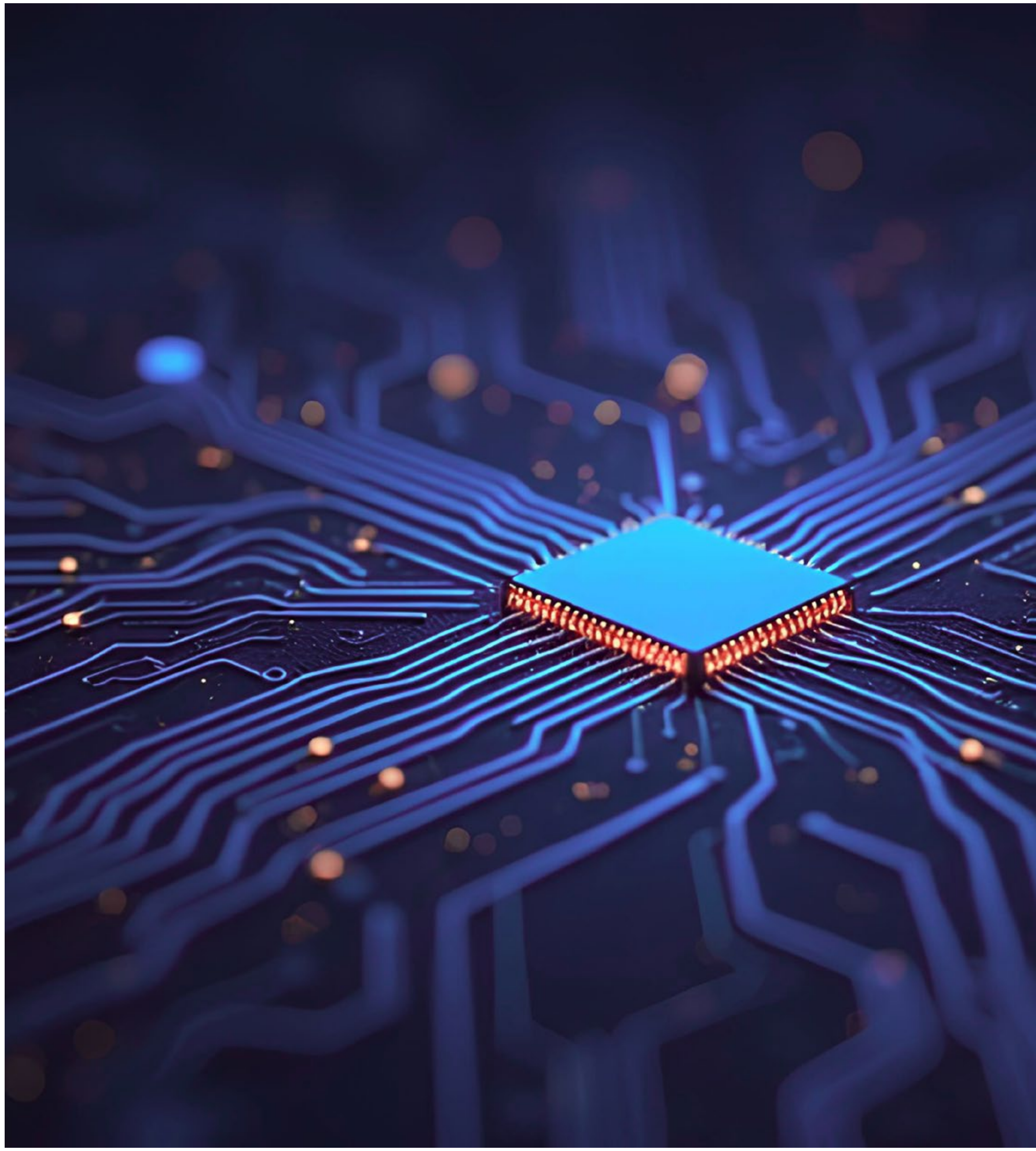
This report is organised into chapters, each highlighting a significant topic from 2025 – whether it's an emerging threat, a notable trend, or a critical development in cybersecurity. To make the content actionable and easy to digest, every chapter follows a consistent structure:

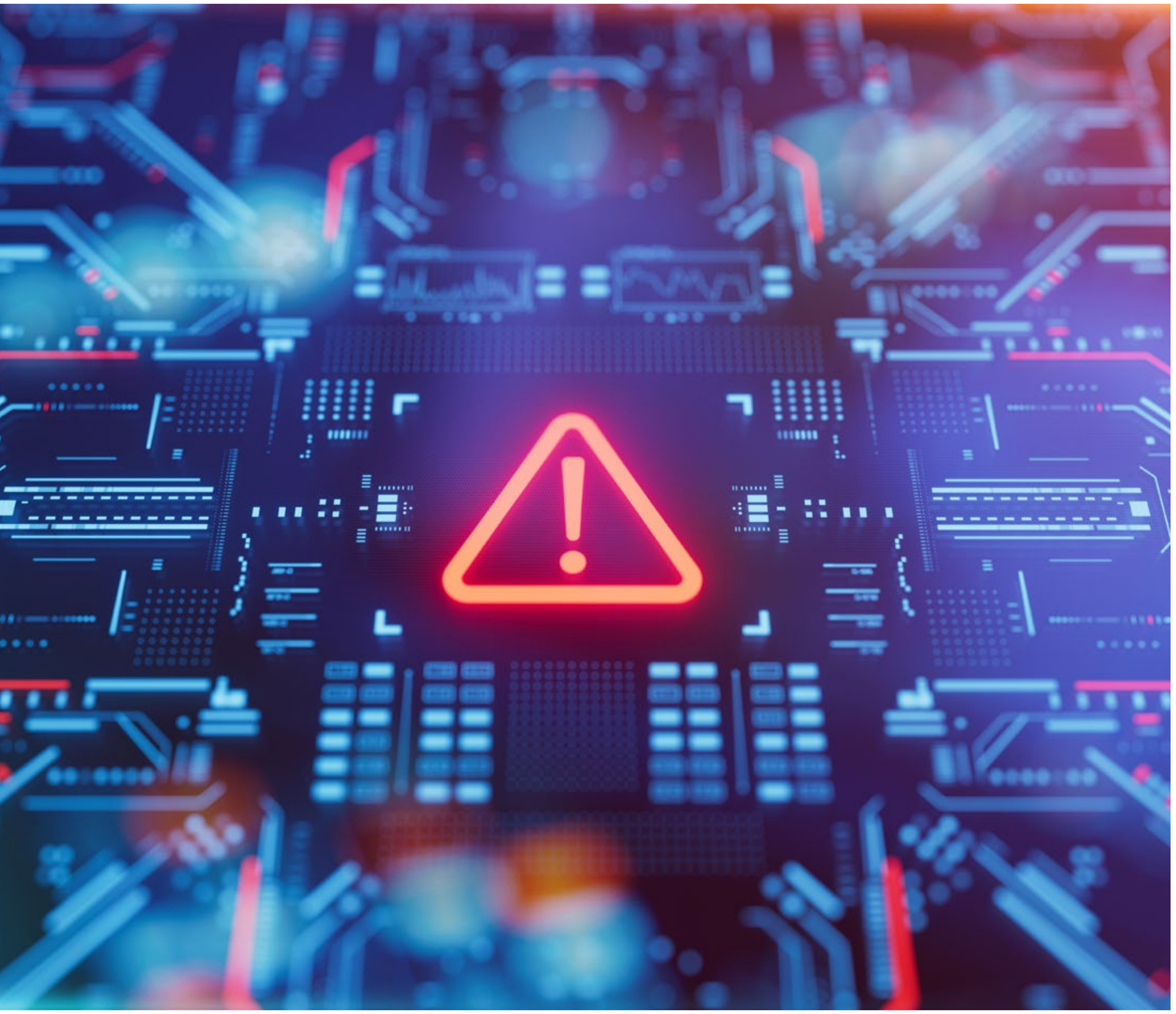
What You Need to Know
A clear explanation of the topic, including its context and relevance.

Why It Matters to You
Insight into the implications for organisations and the broader cybersecurity landscape; why this topic is significant and how it influences the security environment.

Sopra Steria's Recommended Actions
Practical steps and strategies to mitigate the threat or address the trend discussed in the belonging chapter.

Please note that some recommendations may appear across multiple chapters. This is intentional: many mitigation strategies are not limited to a single threat category. They provide broad protection, strengthen multiple layers of defence, and reduce systemic risk across the organisation.





01. EMERGING THREATS

ARTIFICIAL INTELLIGENCE: THE DOUBLE-EDGED SWORD

The rapid evolution of generative AI brings unprecedented opportunities, but also significant security risks. As leading companies such as Google, OpenAI, Anthropic, Meta, and xAI accelerate model development and datacentre expansion, the attack surface grows correspondingly. Emerging players like Mistral, Alibaba Cloud, and DeepSeek further diversify the ecosystem, increasing complexity and potential exposure. Microsoft's integration of AI capabilities into Windows via NPUs adds yet another layer of risk at the endpoint level.

This innovation wave is defined by dramatic advances: up to 99.9% cost reduction, 90% fewer hallucinations through Retrieval-Augmented Generation (RAG), and a 500x increase in processing capacity, enabling models to handle up to 2 million tokens (equivalent to 1.5 hours of video). Combined with an ecosystem of over 10,000 models and flexible deployment across mobile, PC, and cloud environments, these improvements significantly expand the scale and complexity of AI adoption. This growing complexity amplifies operational opportunities but also introduces new security challenges that organisations must address.

> "The rapid evolution of generative AI brings unprecedented opportunities, but also significant security risks.

One example is the introduction of interoperability standards such as Model Context Protocol (MCP). While MCP enables seamless cross-platform implementations, it also creates new vectors for exploitation. Sopra Steria has already observed malicious MCP packages designed to harvest credentials, exfiltrate sensitive data, and compromise local devices.

Advances in multimodal generation further expand the risk landscape. Models capable of generating and manipulating audio, images, and video now make it possible to create highly realistic synthetic content for impersonation, fraud, disinformation, and social-engineering attacks. Video-generation models such as OpenAI Sora 2 and Google Veo 3.1 represent a major shift: where deepfake creation previously required specialised skills, it can now be produced in minutes from a simple text prompt with minimal expertise.

Sopra Steria has observed threat actors adopting generative AI for a growing range of malicious purposes; from social engineering and automating lateral movement within networks, to vulnerability discovery and real-time evasion of security controls.

PromptLock, one of the first identified ransomware groups to leverage generative AI, was discovered using tools such as Claude Code to develop malicious payloads directly on infected systems. Some threat actors have also started using local LLMs on compromised devices to automate post-exploitation activities. Instead of using external command-and-control (C2) infrastructure, attackers can run small, on-device models to analyse local data, and generate malicious scripts.

While this is still in the early phases, Sopra Steria believe that this trend clearly signals how the threat landscape will change. As AI capabilities become increasingly embedded on end-user devices, the barrier for developing and executing such attacks will continue to decrease.

AI Agents for Defensive Operations
AI agents capable of autonomously performing tasks across systems will become an integrated part of future cyber operations. AI agents will eventually play a key role in accelerating detection, investigation, and response.

Today several key security vendors already have virtual agents' capabilities on their platform that use Generative AI to do automated risk assessments, validate security baselines, script detection, but also automated analysis. While many of these platforms are still in the early releases, with the release of new security LLMs, we will see an increase in both accuracy and usefulness of such tools.

Code-Assisted Development
The integration of generative AI into software development workflows has clear productivity benefits, but it also introduces new security risks. LLM-generated code more often contains insecure patterns, outdated libraries, or subtle logic flaws that may not be detected during standard code reviews. In addition, developers may unknowingly paste sensitive data, API keys, or proprietary logic into AI tools, creating data-leakage and IP-exposure risks.

As autonomous or semi-autonomous coding agents gain capabilities, the likelihood of large-scale propagation of insecure code increases. Vulnerabilities introduced by AI-generated components can rapidly spread across repositories, products, or environments, amplifying the blast radius of a single coding flaw. Sopra Steria recommend that organisations need to evolve their secure development lifecycle (SDLC) to include AI-specific code scanning, dependency governance, and model-aware security testing.

With the arrival of AI-integrated developer tools like Cursor, Windsurf, and AWS Kiro, Sopra Steria recommends that organisations assess both the associated security risks and the new ecosystems these tools introduce, asking questions such as:

- What kind of language models are being used?
- What kind of services are being used to process data?
- What kind of guard-rails do they have to protect against prompt injection.

SOPRA STERIA'S RECOMMENDED ACTIONS

To address the rapidly changing risk landscape within the use of AI, Sopra Steria recommend that organisations should adopt a proactive and structured approach to AI security:

Implement AI-specific governance and risk management frameworks, including model access control, data-use policies, and AI supply-chain vetting.

Introduce protective guardrails for AI-assisted development, including code-quality validation, secure coding requirements for LLM-generated output, and mandatory review of AI-produced code.

Ensure users are trained to identify and respond to AI-generated or manipulated content through continuous awareness and detection programs.

When developing custom AI agents, enforce least-privilege access to data and systems, and implement robust safeguards against prompt injection and other manipulation techniques.

Organisations that combine policy, technology, and security-by-design principles will be better positioned to adopt generative AI at scale without amplifying operational or cyber risk. The maturity of AI-driven threats will continue to accelerate, and security strategies must evolve at the same pace.

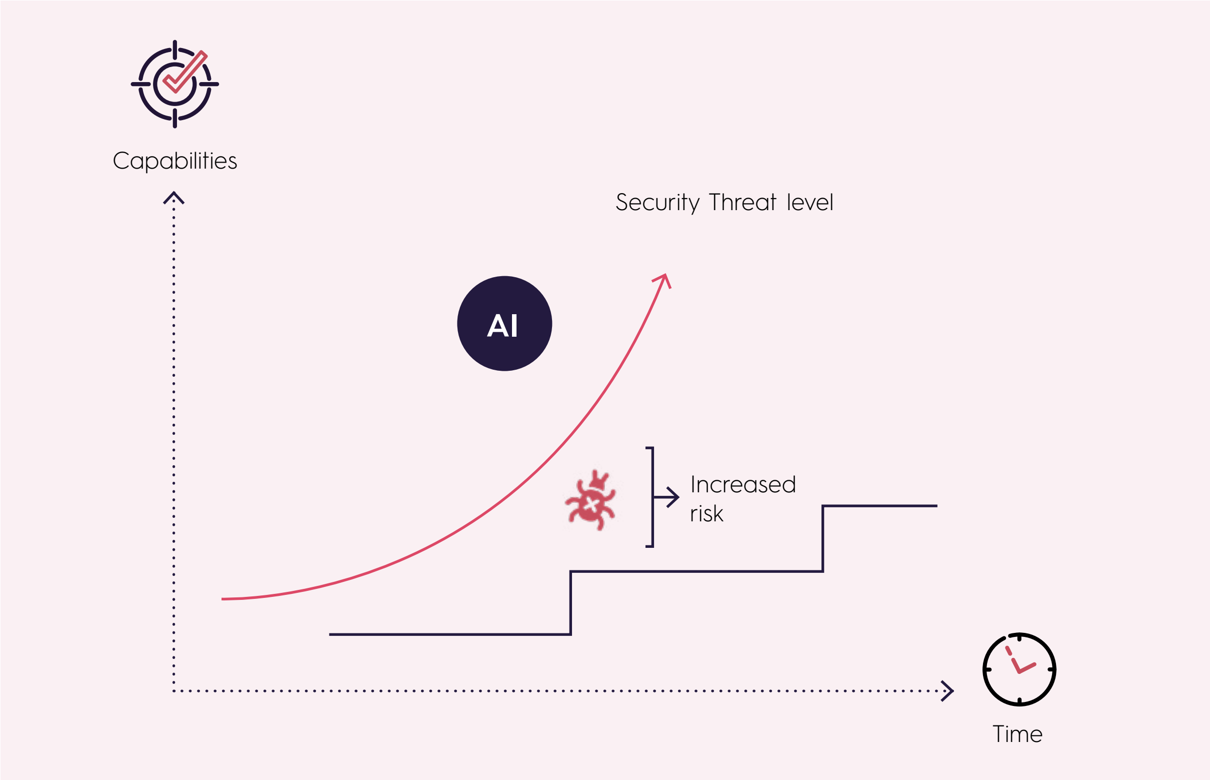
THE EVOLVING CLOUD RISK LANDSCAPE

Cloud and technology drive global business and shapes geopolitics. There is a clear shift, where control of digital infrastructure has moved from companies to global powers. This makes your cloud strategy a political and economic risk decision.

The digital economy now represents about 15% of global GDP, which is more than $16 trillion in 2024 (Global Digital Economy Report 2025, IDCA). At this scale, cloud infrastructure functions as a strategic asset. Policy shifts, trade restrictions, and sanctions increasingly determine which technologies nations and companies can use, turning digital reliance into a geopolitical risk.

At Sopra Steria, we see how regulatory pressure and data-sovereignty requirements are driving architectural fragmentation and higher costs. To stay resilient, we recommend that organisations design for the ability to distribute workloads and data across jurisdictions and providers, ensuring compliance while maintaining performance and control.

Lock-in and traditional operational models struggle to keep up with the evolving threat landscape



> Cloud is no longer solely an IT function. It is a strategic business asset and a critical operational risk that demands board-level oversight, proactive planning, and continuous attention.

Operational Exposure from Foreign Cloud Providers

Reliance on foreign cloud providers introduces exposure to geopolitical and regulatory shifts beyond the organisation's control. Sudden sanctions, export restrictions, or policy changes in a provider's home country can interrupt access to critical systems, sometimes without notice. Even routine updates or maintenance may be influenced by local government priorities, potentially disrupting business operations. These risks necessitate careful mapping of provider jurisdictions and contingency planning to ensure operational resilience.

Compliance and Cost Risks from Fragmentation

Fragmentation arises when organisations must meet different regulatory or data residency requirements across regions. Sovereign cloud mandates that require data to remain within national borders. These mandates may force the migration of data and applications, the restructuring of infrastructure, or the adoption of localised providers, which in turn lead to increased operational complexity, higher costs, longer project timelines, and sometimes reduced functionality when local solutions are limited. Organisations need strategic planning and flexible architectures to mitigate these burdens while remaining compliant.

Strategic Inflexibility Due to Lock-In

Vendor lock-in and over-reliance on proprietary ecosystems reduce strategic flexibility. Lock-in occurs when organisations rely heavily on a single cloud provider's proprietary service. While this can simplify operations initially, it reduces flexibility to respond to shifting market demands, regulatory changes, or provider performance issues. Exiting or switching providers can become costly and time-consuming if applications are tightly coupled to a single ecosystem.

A multi-cloud or hybrid strategy, combined with portable architectures, is essential to preserve strategic agility and avoid dependence on a single vendor. This approach also mitigates concentration risk, avoiding the danger of putting too many eggs in one basket. Recent large-scale cloud outages have revealed how a single provider failure can cascade across regions, disrupting critical national services.

Quantum – The New Security Frontier

Misplaced confidence in cloud security remains one of the greatest risks. Many assume that migrating to the cloud automatically ensures protection, yet cloud security is a shared responsibility; cloud providers secure the infrastructure, but customers must safeguard configurations, access, and data.

Now, a new and disrupting security frontier is emerging. Quantum Computing and Confidential Computing represent opposing forces: one capable of breaking today's encryption, the other designed to protect data even while it's being processed.

Quantum Computing threatens to render current cryptographic methods obsolete, potentially exposing stored data in the future, making the information accessible to anyone. Most cloud providers, including AWS, Azure, and Google Cloud, still rely on classical encryption. Preparing for a quantum future requires migrating to post-quantum cryptography, designed to withstand quantum attacks.

In contrast, Confidential Computing creates a protected environment in the cloud, like a digital safe, so sensitive information can be handled without being exposed to the provider, other tenants, or even system administrators. This opens important opportunities for the future of cloud computing. Organisations can safely work with highly sensitive data, such as financial records, healthcare information, or intellectual property, without risk of exposure.

Cloud Threats in Summary

In short, cloud risk is no longer only a technical challenge, it is an issue of national resilience, economic stability, and strategic independence. Sopra Steria believes that organisations that embrace diversification, flexibility, and risk awareness will be better positioned to withstand the next wave of disruption.

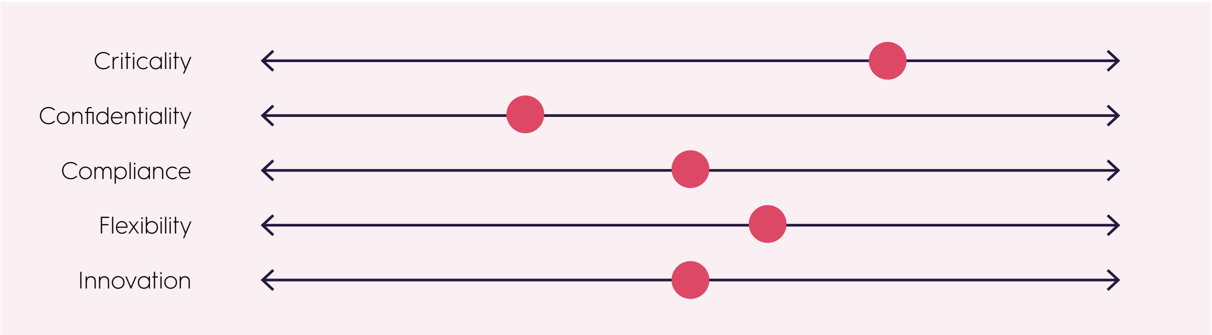
SOPRA STERIA'S RECOMMENDED ACTIONS

Sopra Steria recommends to separate fear from reality. Apply critical thinking: question assumptions, evaluate information sources, and challenge narratives that may be driven by hype or opportunism. Focus on what truly matters to understand what impacts you.

You must have a clear understanding of your risks and dependencies. Begin by mapping your environment, identifying and classifying your data and services, and defining both their criticality, confidentiality, as well as which laws and regulations apply. Then assess the policies of each cloud provider, including sovereignty and how they handle sensitive data and their potential exposure to sanctions or regulatory changes.

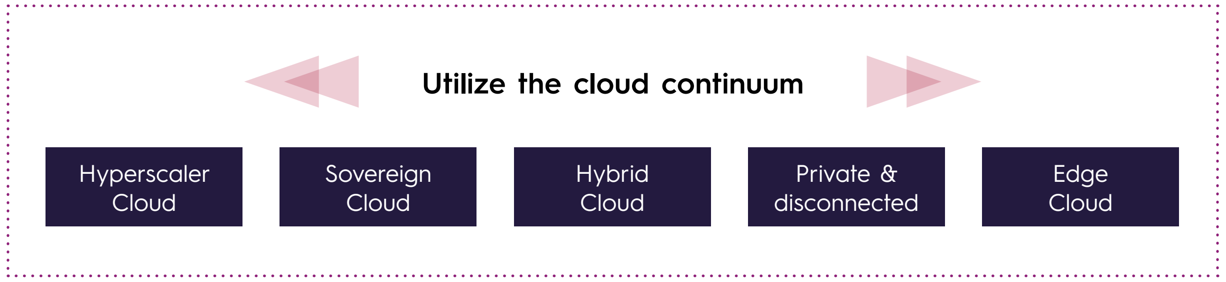
Prepare for Sovereign Cloud readiness by selecting providers that meet data residency requirements and comply with local staffing mandates.

The context you operate in is constantly changing and you need to be able to adapt

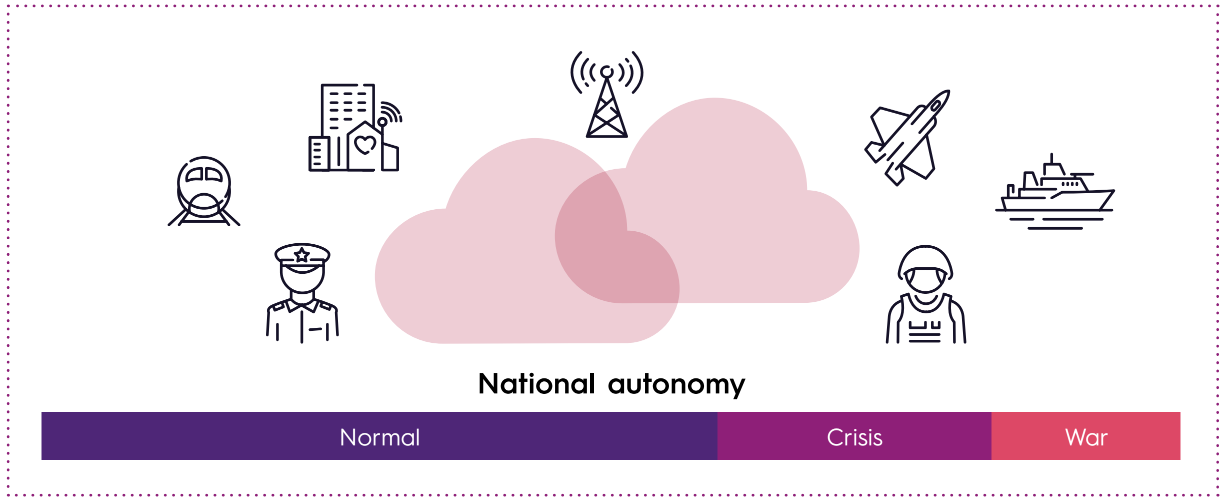


Sopra Steria advises organisations to use the full Cloud Continuum to stay compliant and agile. Combine public, hybrid, and private cloud models, rely on air-gapped setups for your most sensitive systems. Make architecture designs that avoid geographic and technological single points of failure.

Be able to build your flexibility and portability across the cloud continuum



You need to be able to operate your services regardless the state of your nation



Improve portability by using cloud-agnostic tools like Kubernetes and containerization to maintain flexibility. Start exploring unified data platforms that also makes data portable across the continuum. Minimise vendor dependency and avoid deep proprietary lock-in. Favor open standards and abstract cloud services using middleware or orchestration tools, which again can improve portability and reduce migration friction.

Resilience should be in your DNA. Building organisational robustness is about preparing your company to withstand disruptions while maintaining critical operations. Develop a crisis and ransomware response plan that clearly defines roles, responsibilities, and escalation paths. Adopting a minimum viable company approach helps ensure operational continuity under any cloud-related disruption. Identify the essential personnel, systems, and processes needed to sustain operations, reduce unnecessary dependencies, and simplify infrastructure to focus on core business continuity. Build a competent and resilient organisation. Cultivate teams with expertise not only in cloud architecture, security, compliance, and incident response, but also in leadership and organisational preparedness. Strengthening both technical and leadership skills reduces operational and strategic risk, enhances decision-making, and reinforces overall organisational resilience.

National Autonomy. If your business is subject to national regulations for critical infrastructure, you must ensure the availability of essential services and resources in accordance with national laws, even during times of crisis or war.

Achieving technical robustness requires resilient, well-structured systems designed to withstand failures, attacks, and evolving threats. Have a plan B; be prepared for a worst-case scenario. Segment production, development, and backup environments to limit incident impact. Use immutable and isolated backups, stored across separate regions or providers. Encrypt data and backups, prepare for quantum-safe standards.

Confidential Compute can further strengthen protection by keeping data secure even while it's being processed in the cloud, ensuring sensitive information remains private throughout its lifecycle.

02. NORDIC THREAT LANDSCAPE

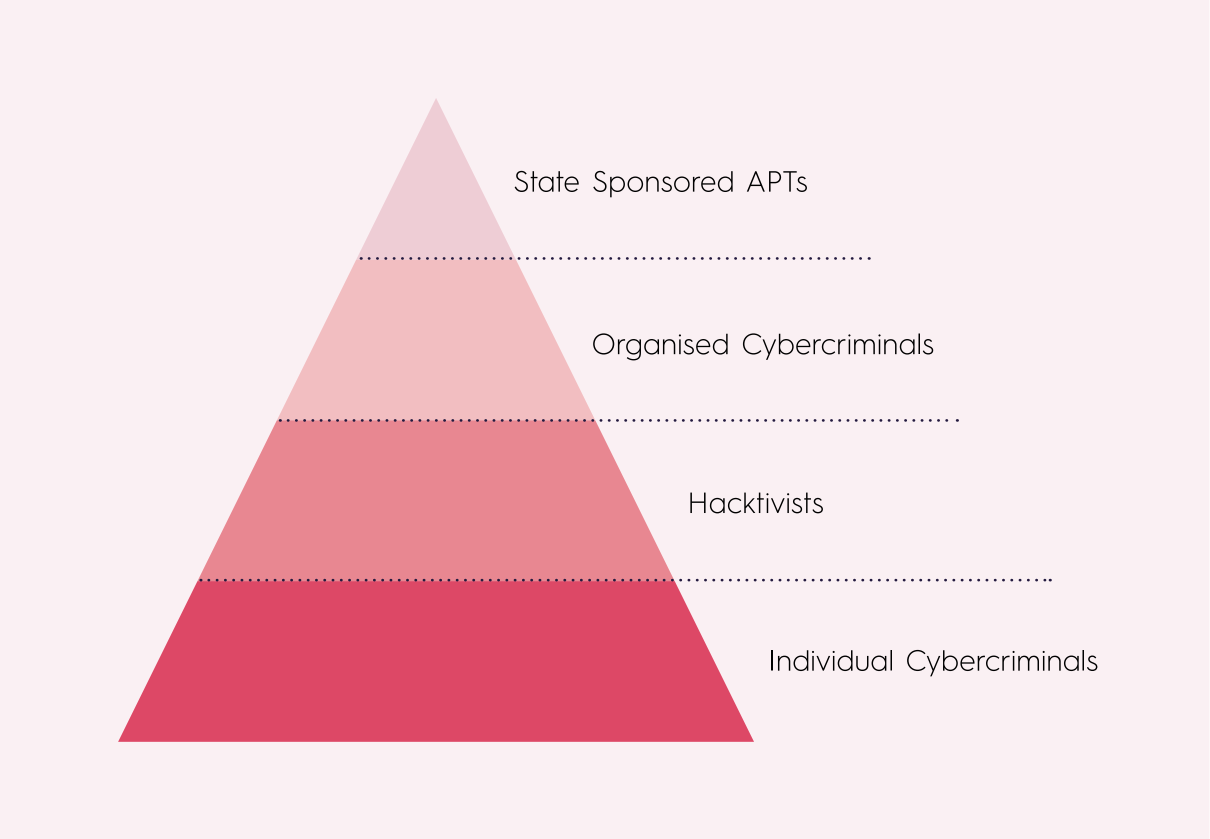
The Nordic region faces a rapidly evolving and increasingly complex threat landscape, driven by the intersection of cybercrime, state-aligned operations, and shifting geopolitical dynamics. Financially motivated attacks remain the main motivation, but the region's strategic position, its proximity to Russia, and the Arctic, combined with NATO's northern expansion, has elevated the Nordics as a highly likely target for state-sponsored campaigns. These developments mean that organisations are no longer dealing with isolated cyber incidents; they are operating in a security environment shaped by global power competition and hybrid threats.

Understanding the Nordic threat landscape is essential for strategic decision-making. Geopolitical tensions influence targeting patterns, attack sophistication, and the likelihood of coordinated campaigns that blend cyber operations with physical sabotage and disinformation. Without a clear view of these risks, organisations may underestimate their exposure and fail to prepare for cascading impacts across sectors.

WHO IS TARGETING THE NORDICS?

The Nordic threat landscape is exposed to risks from all tiers of the threat actor pyramid. Sopra Steria assesses that the most relevant threat actors are state-sponsored Advanced Persistent Threat (APT) groups, cybercriminal organisations, and hacktivists.

The Threat Actor Pyramid



State Sponsored APT

State-sponsored APTs sit at the top of the threat pyramid due to their advanced capabilities, substantial resources, and strategic objectives that often target critical infrastructure and national security. These types of actors are key contributors to the Nordic threat landscape, leveraging substantial resources for espionage, intellectual property theft, and the disruption of critical infrastructure. These actors, primarily from Russia, China, Iran, and North Korea, conduct comprehensive reconnaissance and maintain a persistent presence, underscoring the complexity and severity of the threat environment. Russian and Chinese groups have a long history of targeting Nordic entities for espionage, mapping future attack targets, stealing data, and gaining policy insights. These actors are anticipated to be responsible for the majority of state-sponsored cyber operations in the Nordics in the near future.

> "The Nordic region faces a rapidly evolving and increasingly complex threat landscape, driven by the intersection of cybercrime, state-aligned operations, and shifting geopolitical dynamics.

The Nordic region has become an area of increasing interest for state-sponsored APTs activity, shaped by escalating geopolitical tensions, the war in Ukraine, and its critical role in NATO and European energy security. State-aligned actors remain highly active, targeting government institutions, defence, critical infrastructure, and strategic industries.

Russia

Russian groups have adopted a more aggressive posture, employing hybrid tactics that combine cyber operations, physical sabotage, and influence campaigns. These activities often remain below the threshold of armed conflict and frequently leverage criminal proxies to maintain plausible deniability. Norway's and the broader Nordic region's support for Ukraine, coupled with their strategic position in Europe's energy supply chain, make sectors such as energy, telecommunications, and transport prime targets for espionage and sabotage.

China

China's cyber operations are guided by long-term strategic ambitions: acquiring advanced technologies, establishing footholds in critical infrastructure, and shaping political narratives to support its interests. Chinese actors increasingly blend overt and covert tactics. They combine economic investments, legal business activities, and digital influence campaigns, to secure positions in Arctic development, and embed themselves within Nordic supply chains.

North Korea

North Korea remains a persistent and adaptive cyber threat, primarily motivated by financial gain (notably through cryptocurrency theft and ransomware) and military intelligence collection. North Korean operations often leverage proxies and partnerships with cybercriminal groups. Russia, with its history of destructive cyberattacks against critical infrastructure during periods of crisis, is likely providing North Korea with expertise and infrastructure, enhancing Pyongyang's offensive capabilities. This collaboration raises the risk of more sophisticated and targeted attacks against Western entities.

Iran

Iran has significantly expanded its offensive cyber capabilities, combining low-level disruptive attacks with influence operations to advance its geopolitical objectives. Iranian campaigns primarily target Israel and Western powers, often in retaliation for what Tehran perceives as foreign interference and incitement of domestic unrest, while simultaneously deepening strategic ties with Eastern allies, particularly Russia. Despite differing narratives, Iran's core objective remains retaliation and the strengthening of its regional influence. While Iranian cyber activity persists globally, its overall threat level in the Nordic region is notably lower than that posed by China, Russia, and North Korea.

The boundaries between peace, crisis, and conflict are increasingly blurred. Hybrid operations, which combine cyberattacks, sabotage, and cognitive warfare, are now expected and have evolved into a standard component of the current threat landscape. To counter these risks, reports call for a whole-of-society approach: strengthening civil-military cooperation, harmonizing Nordic and EU regulations, investing in resilience and redundancy, and ensuring that public and private sectors are prepared for scenarios that, until recently, seemed unthinkable.

Cyber Criminals

Cybercriminals occupy the middle tier of the threat pyramid and, though less resourced than state-sponsored actors, remain highly organised and advanced, posing significant risks through financially driven and opportunistic attacks.

Sopra Steria observes that cybercrime in the Nordics is evolving rapidly, becoming more organised and professionalised. Services such as Ransomware-as-a-Service (RaaS), Infostealer-as-a-Service (IaaS), and Initial Access Broker (IAB) have lowered barriers to entry, enabling even low-skilled actors to launch sophisticated attacks.

Cybercriminal organisations have evolved into highly structured, professional networks. Rather than managing the entire attack chain themselves, they operate with specialised teams focused on distinct stages, such as initial access, malware development, or infrastructure management. These groups are hierarchically organised, with clear roles and responsibilities, and some even maintain HR departments for recruitment, onboarding, and performance management. Functioning like cartel-style enterprises, owner-groups coordinate multiple specialised teams, collaborate across borders, and partner with other criminal organisations and state-sponsored APTs.

Sopra Steria assesses that cybercriminal threats pose a risk to every organisation in the Nordics. Cybercriminals are opportunistic, focusing on easy and profitable targets; exploiting weak controls, poor visibility, and delayed patching. Their decentralised operations mean attacks can strike from anywhere, at any time.

In 2025, ransomware has become professionalised, operating like a mature business ecosystem. Credential theft and session hijacking are now the main entry points for both financially motivated and state-aligned actors, allowing them to bypass controls and infiltrate critical systems. According to published reports, Europe accounts for nearly 22% of global breach victims, with Sweden ranking ninth in Europe among the most targeted countries.[1]

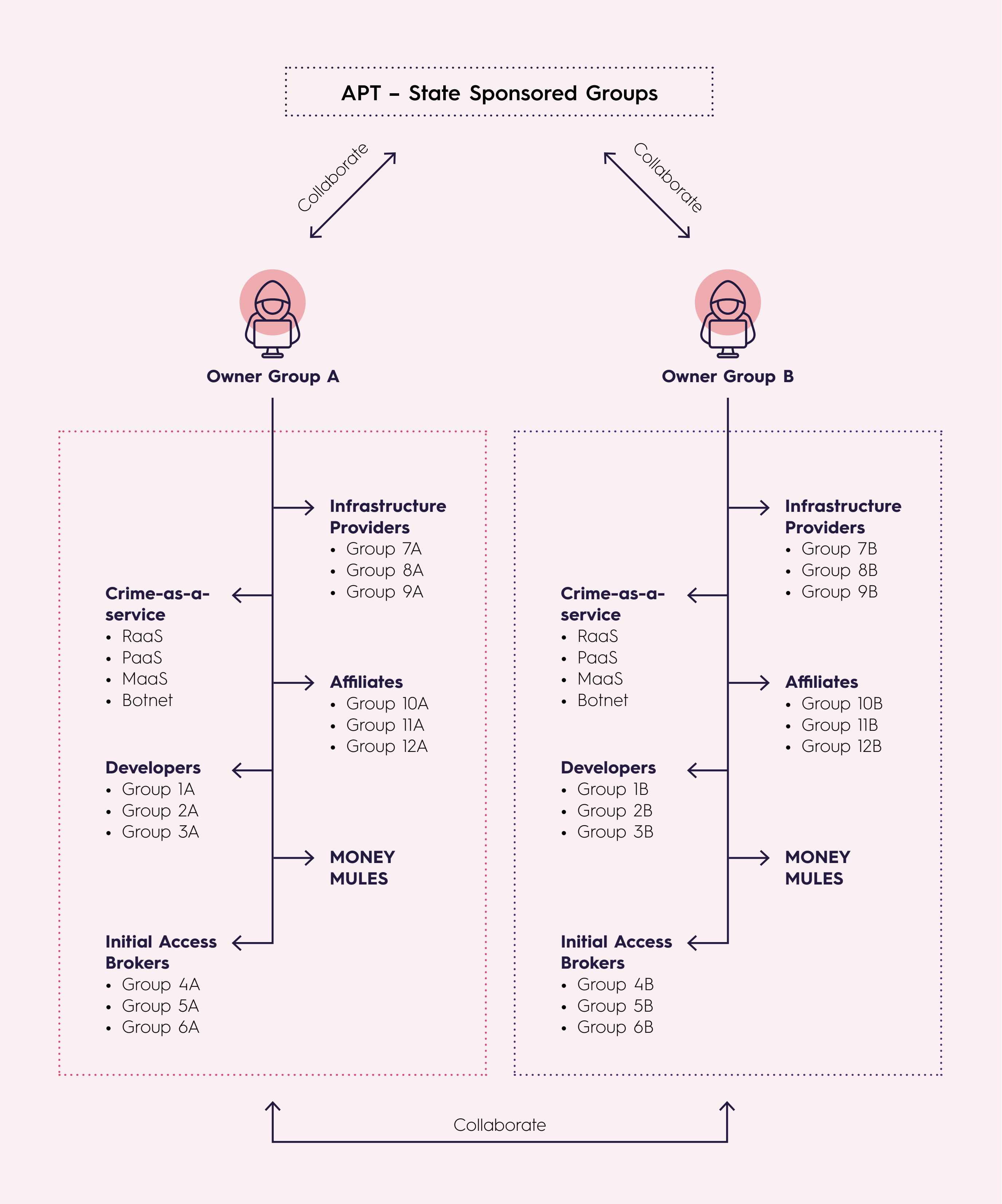
Hacktivists

Hacktivists occupy the lower tier of the threat pyramid and, while lacking the resources and capabilities of more advanced actors, they remain motivated and can cause disruption through opportunistic attacks driven by ideological or political agendas.

Hacktivist groups contribute to large volumes of DDoS and defacement attacks, often timed around political events or societal issues. Many hacktivist personas serve as a cover for state-aligned operations, a phenomenon known as "faketivism". Proxy actors are increasingly used for sabotage and influence campaigns, extending state reach while masking attribution. These campaigns are amplified by artificial intelligence, deepfakes, and coordinated disinformation efforts designed to polarize societies, undermine democratic processes, and erode confidence in institutions.

Beyond financial and espionage-driven intrusions, Sopra Steria observes that influence operations remain a persistent threat. Influence operations and hacktivist activity endure, leveraging DDoS attacks and disinformation campaigns to amplify social polarisation.

Illustration of how cybercriminals are organised



[1] https://www.crowdstrike.com/en-us/resources/reports/2025-european-threat-landscape-report/

SECTORIAL EXPOSURE

Across Europe, cyber threat actors increasingly concentrate on sectors that underpin critical infrastructure, and the Nordic region is no exception. Sopra Steria observed that a broad range of industries were affected last year.

Energy and Telecom

The petroleum sector, particularly in Norway, remains a high-value target due to its role as a key energy supplier to Europe. While reported incidents are relatively few, this is likely due to strong sectoral resilience and underreporting rather than lack of adversary interest.

State-sponsored groups, particularly from Russia and China, prioritise espionage, sabotage, and long-term pre-positioning within critical infrastructure. Their tactics include cyber operations, intelligence gathering, and increasingly physical infiltration. Infrastructure such as pipelines, undersea cables, and cross-border fibre connections are especially vulnerable to both cyber and physical sabotage. Intelligence assessments indicate that Russia is developing capabilities to threaten Western undersea infrastructure, which is vital for both energy supply, and digital communications in the region.

Hybrid threats, blending cyber and physical attacks, are becoming more common, and sabotage is sometimes disguised as accidental failures. DDoS attacks, especially from pro-Russian hacktivist groups, are increasing in both volume and complexity, targeting telecom providers and energy infrastructure to disrupt services and undermine public trust.

The power sector is generally robust, but supporting IT systems often lacks extensive backup and failover capabilities. This means that a successful cyberattack or IT failure could have outsized, cascading effects across society, impacting everything from government operations to emergency services. The attack surface is further expanding as both sectors migrate systems to the cloud and interconnect with other critical domains such as finance, healthcare, and public administration.

Manufacturing

This is one of the most targeted sectors for cyberattacks in Europe and the Nordics, facing persistent threats from ransomware, data theft, and espionage. Ransomware attacks frequently lead to operational disruptions, production stoppages, and significant financial losses. Data breaches are also common, with attackers seeking to steal intellectual property, trade secrets, and sensitive business information. The convergence of IT and OT in manufacturing environments has broadened the attack surface, making these organisations more vulnerable to both cybercriminal, and state-sponsored attacks.

Destructive attacks directly targeting OT systems remain rare, but indirect disruptions, such as halting production lines or interrupting supply chain continuity, are increasingly observed. Espionage-driven campaigns, particularly from Russian and Chinese actors, exploit vulnerabilities in digitalised and automated manufacturing environments. These campaigns often use spear phishing, credential theft, and exploitation of IT systems to gain access to sensitive data or disrupt operations.

IT

The IT sector itself is a high-value target, both as a direct victim and as a vector for supply chain attacks. Attackers frequently target IT service providers, software developers, and digital infrastructure to gain access to a wide range of downstream clients. Supply chain compromises, such as the insertion of malicious code into software updates or exploitation of third-party vendors, have led to widespread incidents affecting multiple organisations. The sector also faces persistent threats from ransomware, credential theft, and APT actors seeking to steal data or disrupt services.

> "Across Europe, cyber threat actors increasingly concentrate on sectors that underpin critical infrastructure, and the Nordic region is no exception.

Finance

The cyber threat level facing the Nordic financial sector remains high but stable. Cybercriminals groups are the most significant and persistent threat. Their attacks are opportunistic, adaptable, and increasingly sophisticated, often involving credential theft, phishing, and extortion. State actors are active in the region, but their direct impact on finance has been limited; however, geopolitical tensions and dependencies on other sectors (such as cloud and energy) mean indirect risks remain.

The most significant cyber threat to the sector comes from organised cybercriminals. Banks and financial institutions are persistently targeted by DDoS attacks, data breaches, and extortion. The finance sector is the fourth most targeted in the EU, and attacks on payment systems can have ripple effects across the broader economy. Event-driven DDoS attacks by hacktivist groups have become a routine part of the threat landscape facing the Nordic financial industry.

> "Public administration is now the most targeted sector for cyberattacks in Europe, accounting for 38% of all reported incidents in the EU.

Public Administration

Public administration is now the most targeted sector for cyberattacks in Europe, accounting for 38% of all reported incidents in the EU. The vast majority of attacks are hacktivist-led DDoS campaigns (96.2% of incidents in this sector), often timed around elections, high-visibility events, or political decisions (e.g., support for Ukraine)[2].

Sopra Steria observed that the pro-Russian group NoName057(16) escalated DDoS attacks on NATO-aligned countries and specifically targeted Norway in connection with the 8th of September 2025 parliamentary election. These attacks were publicly claimed via Telegram. These developments demonstrate that DDoS is no longer merely disruptive, it has become a strategic tool for influence and destabilisation.

Government agencies and municipalities remain high-risk targets. Hacktivist-led DDoS campaigns are often timed with elections and political events to disrupt services and erode public trust. These operations are frequently amplified through coordinated social-media narratives and increasingly paired with ransomware and data breaches, especially against smaller public entities with limited resources and lack of modern systems.

State-aligned actors from Russia, China, Iran, and North Korea are persistently targeting government, defence, and critical infrastructure, using both cyber operations and influence campaigns.

Transport and Logistics

The transport and logistics sector in Europe and the Nordics is among the most targeted for cyberattacks, with rail and aviation systems holding strategic importance for national security and NATO's northern frontier. This makes them especially attractive targets for espionage-driven campaigns. Most incidents involve hacktivist-led DDoS attacks, often timed with political events or announcements of support for Ukraine, aiming to disrupt air, rail, maritime, and logistics services and undermine public trust. Ransomware is also a major threat. The maritime sector is exposed to espionage and interference with navigation systems, frequently attributed to Russian and Chinese actors.

Recent campaigns linked to Russian actors have specifically targeted logistics and military mobility, using spear phishing, credential theft, and exploitation of IT systems to compromise operational readiness. The increasing digitalisation and automation of transport systems have improved efficiency, but also widened the attack surface, making these systems more vulnerable to both cybercriminal and state-sponsored attacks.

Healthcare

The Nordic healthcare sector faces a persistently high cyber threat level, driven by both financially motivated actors and state-aligned groups. Hospitals and healthcare services are prime targets for ransomware and data theft, with attacks disrupting patient care and exposing sensitive information. The sector is particularly attractive because prolonged system outages can be life-threatening, making organisations more likely to pay ransoms to avoid risks to patient safety, even death. Foreign states are assessed as highly likely to pursue espionage, targeting health data, research, and crisis management capabilities, while hacktivists continue to launch DDoS attacks linked to geopolitical events such as the war in Ukraine.

Heavy reliance on outdated systems, complex digital value chains, and underfunded cybersecurity measures amplifies exposure, while even minor disruptions in treatment or distribution can have severe societal consequences.

[2] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

Education and Research
Norwegian technological research, development, and production are of significant interest to foreign threat actors. Technical and scientific knowledge often has dual-use potential, enabling military advancements. Access to laboratories, specialised equipment, and training in instrumentation is as sought after as theoretical expertise. The Norwegian Intelligence Service has reported cases where researchers from China and Iran, affiliated with Norwegian universities, also work for entities in their home countries involved in developing military technology. The most exposed research areas include semiconductor and sensor technology, material science, cryptology, IT security, biotechnology, and artificial intelligence.

The research and development sector faces persistent attempts at illegal knowledge transfer. Unlike physical goods, the transfer of knowledge that can enhance military capabilities is less strictly regulated, making it a prime target. Universities and research institutions are frequent victims of phishing, credential theft, and cyber espionage, driven by both cybercriminals and state actors seeking intellectual property and access to broader networks.

Water and Wastewater
Water and wastewater utilities are increasingly recognised as critical infrastructure in the Nordics, yet they remain highly exposed to cyber risk. A successful attack can disrupt essential services, compromise public health, and trigger cascading effects across other sectors.

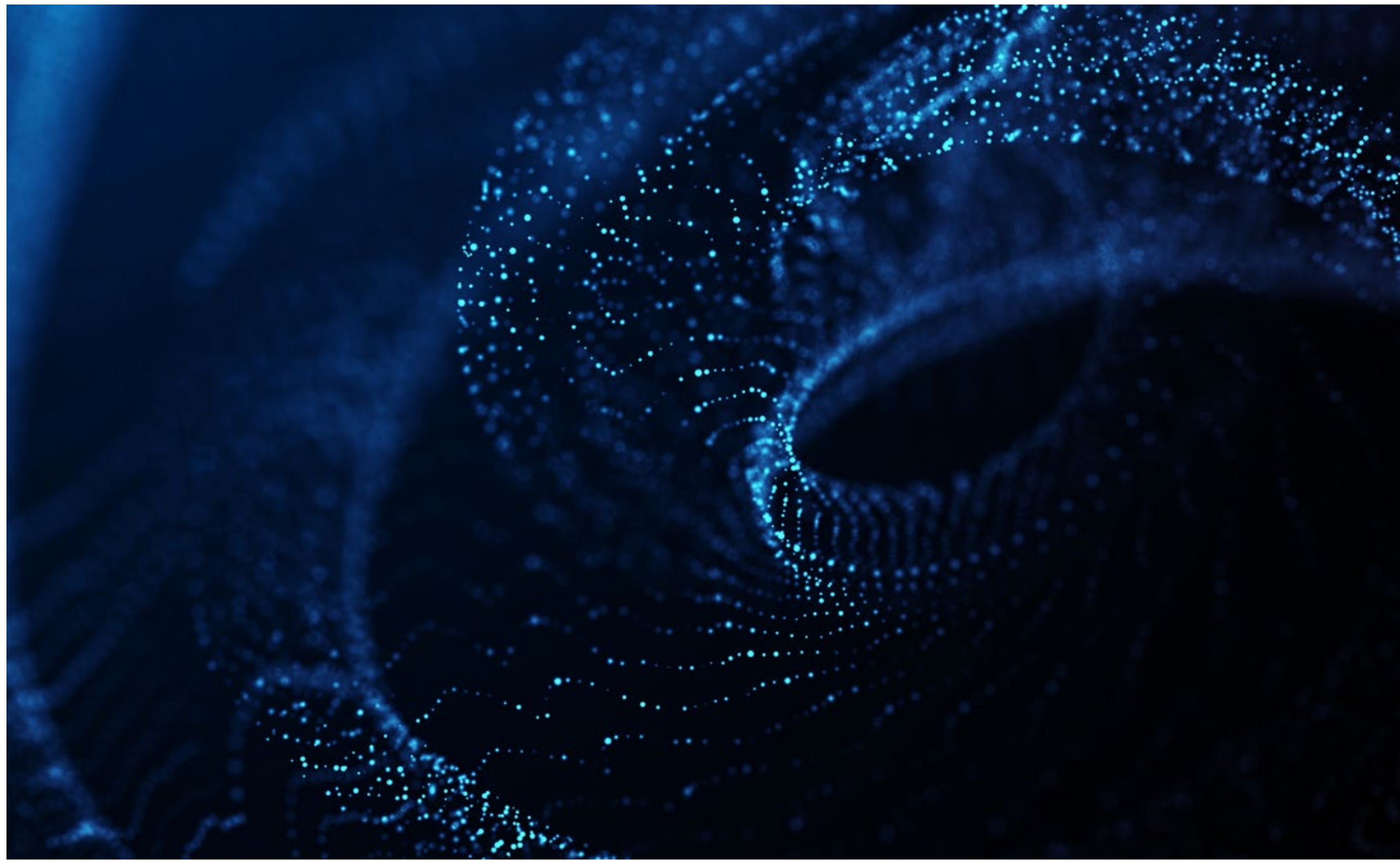
The sector's vulnerability stems from aging control systems with minimal cybersecurity protections, combined with a highly fragmented structure that makes consistent security practices difficult to enforce. Underfunding and a shortage of skilled personnel further compound the risk, meaning even minor disruptions in water treatment or distribution can escalate into serious societal consequences.

WHAT DOES IT MEAN FOR YOUR ORGANISATION?

Cyber threats in the Nordics are not abstract, they directly impact your business operations, financial stability, and reputation. Here's why this matters and what you need to consider:

What's Changing
Cyber threats in the Nordics are becoming faster, more sophisticated, and harder to detect. AI-driven phishing and automated reconnaissance are accelerating attack speed, while criminal groups and state-aligned actors increasingly collaborate, sharing tools and infrastructure. Hybrid operations, combining cyberattacks with physical sabotage and disinformation, are now a persistent reality, creating multi-layered risks that traditional security measures cannot fully address.

Why It Matters to You
These developments directly impact business continuity, financial stability, and reputation. Ransomware can halt operations for weeks, causing severe revenue loss and recovery costs in the millions. Data breaches trigger GDPR penalties and erode customer trust, while attacks on IT systems supporting operational technology can disrupt production and supply chains. Stolen credentials remain a critical entry point for attackers, enabling privilege escalation and large-scale compromise. Geopolitical tensions amplify these risks, making Nordic organisations prime targets for espionage, sabotage, and influence campaigns that can destabilise operations and public trust.



SOPRA STERIA'S RECOMMENDED ACTIONS

> "Cyber threats in the Nordics are becoming faster, more sophisticated, and harder to detect.

Understanding the evolving threat landscape is critical for building resilience. The Nordic region faces a combination of geopolitical, economic, and technological risks that demand a proactive, whole-of-society approach. Organisations should prioritise the following:

Map Your Sector's Risk Profile
Identify how your industry is exposed to cyber threats. Understand your key assets, supply chain connections, and operational interdependencies that could amplify the impact of an attack.

Understand Who Is Targeting You
Recognise the threat actors relevant to your organisation (state-sponsored groups, organised cybercriminals, and hacktivists), and understand their motives and methods.

Monitor Geopolitical Drivers
Stay informed about global and regional developments that could shift threat priorities or increase risk to your sector.

Build Intelligence-Driven Defences
Leverage actionable threat intelligence tailored to your industry and collaborate with partners to strengthen collective security.

Plan for Resilience and Redundancy
Prepare for disruption by implementing robust contingency plans, ensuring system redundancy, and aligning with regulatory requirements.

Technical Mitigations
For guidance on specific mitigations against attack vectors in the kill chain, refer to Chapter 3: Sopra Steria's SOC Observations.

03. SOPRA STERIA'S **SOC OBSERVATIONS**

INITIAL ACCESS

In 2025, Sopra Steria observed threat actors using a broad set of familiar techniques for initial access. While phishing remains a leading attack vector in the Nordics, a clear shift is underway. Modern campaigns have evolved beyond basic phishing into complex, multi-stage strategies combining technical exploits, social engineering, infrastructure manipulation, and stealth tactics via legitimate platforms. Rather than forcing entry, attackers aim to blend into normal activity, leveraging trusted tools and common user behaviours to infiltrate systems quietly and bypass traditional detection.

> "The trend is unmistakable: Attackers don't break in – they log in.

Credential Harvesting

Credential harvesting remains a core objective across attack campaigns. Adversaries leverage phishing, infostealer malware, and password spraying to capture usernames, passwords, and authentication tokens – assets that are quickly monetised on dark web markets. These stolen credentials fuel a thriving cybercrime economy and enable cascading attacks such as ransomware, data exfiltration, business email compromise, and extortion. The trend is unmistakable: attackers increasingly log in rather than break in.

Phishing

Phishing continued to dominate as one of the leading initial attack vectors observed in Sopra Steria's customer base throughout 2025, mirroring global trends.

Sopra Steria Scandinavia observed that 44,4% of all security incidents within their customer's base were phishing related.

In 2025, fake CAPTCHA pages became a major phishing trend, with attackers using them to make malicious sites appear legitimate and evade automated security checks. These deceptive prompts often lead users to credential-harvesting pages or malware downloads, exploiting the trust placed in CAPTCHA as a security feature.

The rise of Phaas, and other cybercrime toolkits has lowered barriers, enabling large-scale campaigns even by novices. These platforms combine ready-made kits, infrastructure, and automation with AI-generated targeting and lures, enabling phishing campaigns with click-through rates up to four times higher than traditional attempts.

The Rise of ClickFix

ClickFix has surged as a leading initial access technique, overtaking phishing globally and now driving 47% of attacks.[3] This social-engineering tactic tricks users into pasting malicious commands (often delivered through fake pop-ups or job applications) into Windows Run or terminal windows. Doing so triggers PowerShell or mshta.exe to load payloads filelessly and evade traditional defenses. Its appeal lies in bypassing phishing controls and exploiting user actions, enabling malware delivery, credential theft, and persistent access with minimal effort. Both cybercriminals and nation-state actors are leveraging ClickFix, and while phishing still dominates in the Nordics, adoption of this method is rising fast.

[3] Microsoft Digital Defense Report 2025

Adversary-in-the-middle
AiTM attacks are escalating in scale and sophistication, targeting cloud identity systems and authentication flows. By intercepting session tokens, attackers bypass MFA and gain covert, persistent access. Campaigns increasingly combine advanced techniques (such as device code phishing, OAuth consent phishing, and AiTM) to maximise impact. Victims are redirected to sites mimicking legitimate portals, tricked into granting OAuth permissions, and exploited via device code flows, allowing attackers to hijack tokens and maintain access to sensitive accounts.

Business Email Compromise
In 2025, BEC attacks have become more targeted and persistent. Adversaries increasingly use credentials stolen through phishing to access legitimate business email accounts, manipulate ongoing threads, alter payment instructions, and commit financial fraud. Although BEC represents a smaller share of overall threat activity, its financial and operational impact remains severe due to its reliance on identity compromise and convincing social engineering.

Sopra Steria has observed that a successful BEC compromise rarely remains isolated; threat actors rapidly pivot to the victim's partners and third-party vendors, using the compromised account to launch convincing phishing attempts against them. This cascading effect is particularly concerning when viewed against the sheer volume of email traffic organisations handle. Sopra Steria Scandinavia's customer base received more than 635 million emails in their inboxes combined during 2025 (excluding junk and quarantined mails). With an average of 5.5 URLs and 1.4 attachments per mail, which equates to approximately 3.5 billions URLs and 900 million attachments in circulation. This demonstrates the massive volume of URLs and files employees interact with. When BEC actors operate from trusted, compromised accounts, users face an even harder task distinguishing malicious content from legitimate communication.

The Trojan Employee
Cybercriminals are moving beyond traditional hacking, using AI-driven deception to infiltrate companies via remote roles. Threat actors craft hyper-realistic résumés and portfolios with generative AI, fabricate entire career histories, and even deploy deepfake video interviews to impersonate skilled candidates. Automated hiring systems can be easily misled by AI-optimised applications, and reduced physical verification in remote-work settings further complicates detection. Once hired, these "Trojan employees" gain insider access to sensitive systems, turning trust into a vulnerability. Several European firms, including cases in Norway, have fallen victim, with investigations linking many operations to North Korean actors. Additionally, throughout 2025, there have been multiple instances where threat actors bribed employees to disclose sensitive information or provide login credentials in exchange for money.

!

Key Red Flags To Look Out For:

Camera Avoidance
The candidate claims there are issues with their camera, never turns it on, or consistently finds excuses to avoid video calls.

Deepfake Risk
The candidate's video presence or documents may use deepfake technology to impersonate someone else.

Unusual Behaviour
They complete work tasks satisfactorily but avoid personal interaction or verification steps.

Geographic Inconsistencies
The candidate logs in from suspicious or unexpected locations, which don't match their claimed country of residence.

Accent and Appearance Mismatch
Their language, accent, or appearance does not align with the country or region they claim to be from.

Call Centre Environment
The candidate appears to be working from a call centre or similar shared workspace, which may indicate organised fraudulent activity.

Supply Chain Attack
Supply chain attacks surged in 2025, growing in both frequency and impact. Threat actors increasingly exploited trusted relationships to infiltrate multiple downstream organisations.

Globally, supply chain compromise accounted for 2% of initial access vectors, marking a notable rise.[4] One example observed by Sopra Steria was the Shai-Hulud campaign: two large-scale attacks on the npm ecosystem where hundreds of maintainer accounts were hijacked to publish trojanized packages, stealing developer and CI/CD secrets. The result was widespread credential theft and data exfiltration, which underscores the persistent risk of hidden vulnerabilities in the software supply chain.

Another notable example in 2025 was a supply chain attack targeted Salesforce customers through the Salesloft Drift integration. Threat actors exploited stolen OAuth tokens to gain unauthorised access to Salesforce environments, resulting in the exfiltration of sensitive customer data from hundreds of organisations.

Exploiting Trusted Applications
Threat actors increasingly weaponise trusted tools to gain initial access, bypassing traditional defences by exploiting user trust. A striking example is the PDFeditor Malware Campaign. Attackers disguised credential-harvesting malware as a legitimate PDF editor. Once installed, it enabled extensive compromise, including credential theft, persistent access, and lateral movement. The intrusion required an urgent response involving device isolation, password resets, and domain blocking. The fallout included operational disruption, elevated incident response costs, and heightened regulatory risk.

[4] Microsoft Digital Defense Report 2025

Vulnerability Exploitation

Vulnerability exploitation is another commonly used initial access method and AI is accelerating it. In 2025, discovered and actively exploited flaws surged, while the gap between disclosure and exploitation shrank. AI-powered tools automate scanning, exploit development, and attack execution, enabling attackers to bypass phishing and launch direct code-based attacks on exposed systems. Organisations now have less time than ever to patch before compromise. Threat actors primarily target network-facing vulnerabilities in unpatched or misconfigured systems for remote, scalable access.

The impact of widespread credential theft, operational disruption, and elevated incident response costs underscore the urgency of proactive patching and continuous vulnerability management.

!

Notable Vulnerabilities That Affected Norwegian Organisations in 2025:

SharePoint (CVE-2025-53770)
Critical RCE flaw in on-prem SharePoint servers allowed arbitrary code execution, file access, and data theft; heavily exploited throughout the year.

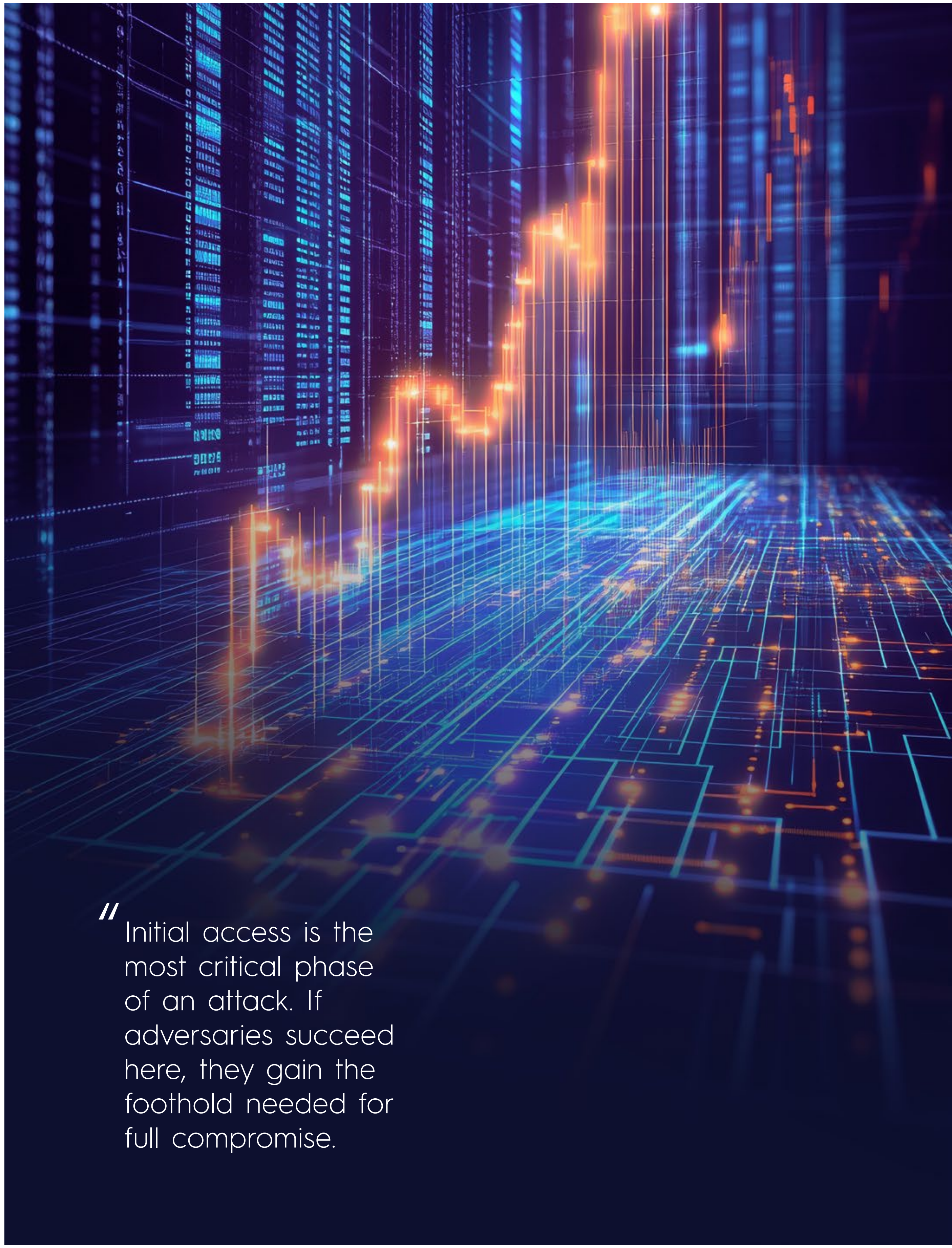
Cisco ISE (CVE-2025-20286)
Static credentials in cloud deployments enabled unauthenticated admin access, data extraction, and service disruption.

Citrix Bleed 2 (CVE-2025-5777)
Severe flaw in NetScaler ADC/Gateway devices allowed session hijacking and token theft; public PoC and confirmed exploitation.

Why It Matters

Initial access is one of the most critical phases in the cyberattack kill chain. If attackers succeed here, they gain a foothold that enables credential theft, lateral movement, and ultimately full compromise. Stopping them at this stage is essential.

The trends shaping initial access in 2025 are not just technical – they represent a fundamental risk to business continuity, reputation, and trust. For customers, the message is clear: attackers are exploiting human behaviour, trusted tools, and identity systems to bypass traditional defences. Relying on legacy security models is no longer enough. Ignoring these trends risks severe financial loss, regulatory penalties, and reputational damage. To stay ahead of evolving threats, organisations must remain vigilant, act decisively, and implement robust mitigation strategies to disrupt attacks at the earliest stage.



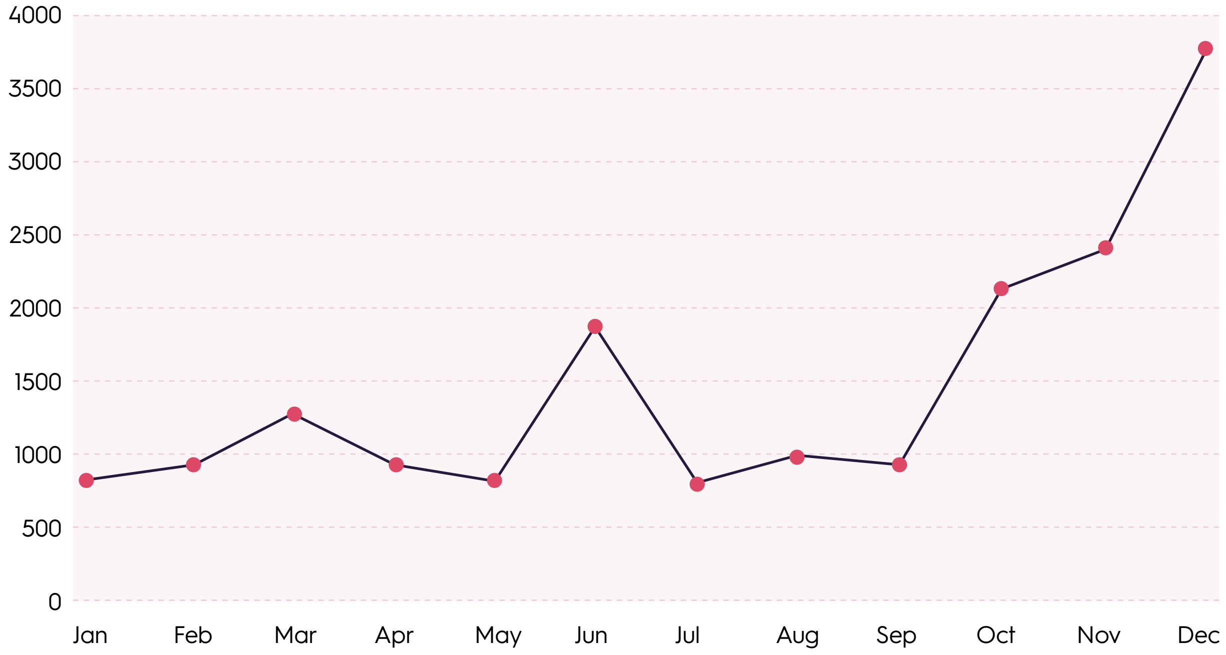
> "Initial access is the most critical phase of an attack. If adversaries succeed here, they gain the foothold needed for full compromise.

POST COMPROMISE

The post-compromise phase in 2025 has become faster, more automated, and significantly harder to detect. Once attackers gain initial access, they move quickly to establish control and expand their reach. Sopra Steria observations show that malware families are increasingly modular and multifunctional. Remote Access Trojans dominate this stage, providing attackers with persistent connectivity and capabilities such as credential theft and remote execution.

Ransomware remains the most disruptive threat, but its delivery has evolved, threat actors now use stealthy loaders and legitimate system tools to avoid detection, while payloads are encrypted and obfuscated to resist analysis. Infostealers and credential harvesters are deployed early to collect browser-stored passwords, cloud tokens, and privileged accounts, enabling rapid escalation.

Malware prevented in Sopra Steria Scandinavia's customer base



> // The post-compromise phase has become faster, more automated, and significantly harder to detect.

Privilege Escalation

Privilege escalation has surged as one of the most exploited tactics in the attack chain. Threat actors increasingly target vulnerabilities in widely used platforms like Windows, Linux, VMware, and cloud services to gain elevated permissions. Microsoft reported that nearly half of all vulnerabilities patched in mid-2024 were privilege escalation flaws, and this trend continued into 2025 with critical exploits in Linux sudo, Windows SMB, and VMware ESXi being actively weaponised. Attackers are also leveraging identity-based weaknesses, misconfigured IAM roles, and hardcoded credentials in SaaS and hybrid environments. Ransomware groups and APT actors combine privilege escalation with lateral movement and persistence to achieve full domain compromise.

Once administrative or root-level control is obtained, adversaries can disable defences, exfiltrate sensitive data, deploy ransomware, and create backdoors for long-term exploitation. The growing number of privilege escalation vulnerabilities highlights systemic weaknesses in patching, identity governance, and configuration management. For enterprises, this means that a single overlooked misconfiguration or unpatched flaw can lead to a full breach. The combination of privilege escalation, cloud adoption, and identity focus increases risk, as attackers leverage trust relationships, identity workflows, unmonitored privilege assignments, or delayed revocation of access to escalate privileges without detection.

Persistence

Since 2024, persistence techniques have evolved, shaped by persistence strategies originating from APT playbooks, cloud adoption, and the increasing sophistication of ransomware groups. Sopra Steria data suggests that attackers are moving away from traditional malware implants toward stealthier methods that blend into legitimate processes. "Living-off-the-land" (LOTL) tactics have become dominant, where adversaries leverage built-in tools like PowerShell, Windows Management Instrumentation (WMI), and scheduled tasks to maintain access without triggering defences. Cloud environments have emerged as a prime target, with attackers adding rogue credentials, roles, and API keys to ensure long-term access. Identity-based persistence, such as manipulating IAM policies or creating hidden admin accounts has accelerated in hybrid and SaaS ecosystems.

Persistence is no longer just about malware; it's about control over identities, configurations, and trusted components. This makes detection harder because attackers increasingly mimic normal administrative behaviour. Traditional endpoint-centric defences are becoming insufficient, and the attack surface now spans cloud platforms, supply chains, and operational technology. The persistence trend also amplifies the risk of long-term espionage and data exfiltration, as adversaries can remain undetected for months or even years, as seen in campaigns by China-nexus groups and the Salt Typhoon operations. For organisations, this means that compromise is not a one-time event, but an ongoing condition unless proactive measures are taken. Attackers aim to stay hidden for as long as possible, making persistence difficult to counter.

Lateral Movement

Lateral movement has become faster, stealthier, and more automated than ever before. Attackers have been observed achieving lateral spread within minutes after initial compromise. This acceleration is largely driven by AI-enhanced attack automation and credential abuse, enabling adversaries to mimic legitimate user behaviour and evade detection. Techniques such as Pass-the-Hash, Pass-the-Ticket, and exploitation of remote services like RDP and SMB remain prevalent, but they are increasingly combined with "living-off-the-land" tactics using PowerShell and WMI. Cloud environments have introduced new attack paths, including container escapes and service account abuse.

Threat actors design campaigns to exploit trust relationships and identity systems. This stealth allows adversaries to escalate privileges, harvest credentials, and reach high-value assets like domain controllers or sensitive data repositories. For enterprises, a single compromised endpoint can rapidly become a systemic breach, amplifying financial, operational, and reputational damage.

C2 & Exfiltration

Attackers have refined C2 operations and data exfiltration techniques to achieve stealth and resilience. C2 channels increasingly leverage legitimate protocols like HTTPS, DNS, and even cloud APIs to blend malicious traffic with normal network activity. DNS tunnelling has become a favoured method, allowing malware to encode commands and stolen data within DNS queries that bypass firewalls. Frameworks like Cobalt Strike and Sliver remain popular in this space, offering modular capabilities for covert beaconing and encrypted payload delivery. Cloud environments and SaaS platforms have introduced new exfiltration paths, with attackers exploiting misconfigured storage buckets and API tokens to steal data silently.

Threat actors increasingly exploit trusted communication platforms such as Telegram, Discord, Slack, and Microsoft Teams for C2 and data exfiltration. These applications provide encrypted messaging, file-sharing capabilities, and APIs that attackers can abuse to relay commands or transfer stolen data. By leveraging these platforms, malicious traffic blends seamlessly with legitimate collaboration activity, making detection challenging. Because these services are widely trusted and often whitelisted, traditional security controls struggle to differentiate malicious use from normal business operations. C2 and exfiltration aims to integrate into normal operations. By relying on trusted services and encrypted channels, attackers bypass traditional perimeter defences and evade signature-based detection.

The financial and regulatory implications may be severe; stolen intellectual property, leaked customer data, and compliance violations can result in monetary losses and reputational damage. The convergence of C2 and exfiltration with ransomware amplifies risk, as attackers weaponise stolen data for extortion and public exposure.

What is Changing?

The post-compromise landscape in 2025 reflects an evolution where attackers prioritise stealth, automation, and identity compromise over noisy exploits. Across all stages, adversaries have shifted from relying on traditional malware implants to identity-centric and cloud-integrated tactics that blend seamlessly with legitimate operations. The expanding attack surface across hybrid infrastructures, cloud ecosystems, and collaboration tools demands a shift from perimeter-based security to adaptive, identity-first defences.

> "Persistence is no longer just about malware; it's about control over identities, configurations, and trusted components.

SOPRA STERIA'S RECOMMENDED ACTIONS

By combining the measures below, organisations can significantly reduce the likelihood of successful attacks across the entire kill chain; from initial access and execution to privilege escalation, persistence, lateral movement, and data exfiltration – thereby strengthening resilience against modern threats at every stage.

Strengthen Identity and Access Controls

- Enforce the Principle of Least Privilege across all accounts, including service and machine identities.
- Implement Privileged Access Management (PAM) and make Multi-Factor Authentication (MFA) mandatory for every access point.
- Continuously monitor for unusual privilege changes and unauthorised credential additions.
- Audit and disable inactive accounts to prevent attackers from targeting stale credentials.
- Audit supply chain and third-party access.

Adopt Zero Trust and Continuous Verification

- Apply Zero Trust principles to validate every user and device interaction.
- Use behavioural analytics and anomaly detection to uncover deviations in user or system behaviour.

Patch Policy

- Separate policies for devices based on their use-case.
  - End-user clients
  - Windows Servers
  - Linux hosts
  - Network equipment
- Implement patch policies for all systems.
- Prioritise internet-facing systems.

Provide Ongoing User Education on

- Phishing, credential hygiene, the risks of pasting unknown commands (e.g., ClickFix attacks), and recognizing social engineering tactics. Perform tabletop exercises regularly.

Establish and Train on an Incident Response Plan

- Develop an incident response and continuity plan that outlines clear roles, responsibilities, and escalation paths for different attack scenarios.
- Regularly validate the plan through tabletop exercises simulating realistic incidents (e.g., ransomware outbreak, insider compromise, supply chain breach).
- During exercises, ensure the following key questions are addressed:
  - Does everyone know what to do if this happens?
  - What mitigations and actions should the organisation take immediately?
  - Who should the organisation contact (internally and externally) for support and escalation?
- Include communication protocols for regulators, law enforcement, partners, and customers as part of the plan.

Enhance Detection and Response Capabilities

- Deploy Extended Detection and Response (XDR) and Endpoint Detection and Response (EDR) to correlate signals across endpoints, networks, and cloud services.
- Conduct proactive threat hunting to identify indicators of persistence, lateral movement, and covert communication channels.

Limit Attack Surface and Movement

- Implement network segmentation, identity-based segmentation, and secure internal communications to restrict lateral movement and protect critical operations.
- Apply strict patching, configuration validation, and application whitelisting to close common escalation paths.

Secure Data and Communication Channels

- Integrate Data Loss Prevention (DLP) with behavioural analytics to detect unauthorised data movement.
- Monitor encrypted traffic for anomalies such as DNS tunnelling and irregular outbound transfers.
- Enforce policies on approved cloud applications and collaboration tools to prevent shadow IT risks.

Maintain and Update an Assets Inventory

- Maintain and update an asset inventory with clear prioritization of business-critical systems.
- Map system exposure (e.g., public interfaces, remote access, third-party connections) across the network architecture.

04. MOBILE DEFENCE SECURITY

MOBILE AS A PRIMARY ENTERPRISE ATTACK SURFACE

Sopra Steria's work across identity, cloud security, endpoint protection, and SOC operations reveals a clear trend: mobile fleets have emerged as a major enterprise risk. Today, 60% of critical enterprise data is handled through mobile devices.

In other words, mobile devices have become the primary interface for business operations. This shift has amplified exposure to mobile threats, which according to Enisa now account for 42.4% of analysed security incidents – the largest share across all categories.

Sopra Steria has observed this threat activity now spans across all four mobile vectors defined in the Mobile Risk Matrix:

Web & Content
Mobile phishing – email, SMS ("smishing"), messaging apps, QR codes ("quishing"), and push notifications – remains the most common initial access vector.
AiTM kits target mobile browsers to steal session cookies and bypass MFA. These behaviours align with MITRE ATT&CK for Mobile techniques such as MFA request manipulation, and credential interception.

Applications
Spyware, surveillanceware, trojans, and malicious SDKs continue to rise. Recent forensic work by Citizen Lab confirmed exploitation of a zero-click iMessage vulnerability by the mercenary spyware vendor Paragon, used to target journalists. OWASP Mobile Top 10 further highlights supply-chain risks from compromised SDKs, insecure update channels and malicious libraries – one of the fastest-growing mobile attack paths.

Device
Attackers exploit outdated operating systems, unpatched vulnerabilities, rooted/jailbroken devices, and unsafe configurations (e.g., USB debugging, sideloaded apps). MITRE enumerates these under privilege escalation, local exploit execution, and malicious configuration profile manipulation.

Network
Mobile devices frequently connect to untrusted networks. Rogue Wi-Fi, fake access points, SSL stripping, malicious VPN configurations and fake base stations allow man-in-the-middle attacks that intercept credentials or inject malicious content.

Across these vectors, the trend is clear: mobile is no longer peripheral. it is a full-spectrum attack surface, increasingly used as the first step in compromising cloud identities and enterprise systems.

> "Mobile risk is an enterprise risk. A compromised phone is often equivalent to a compromised identity.

MOBILE COMPROMISE LEADS DIRECTLY TO IDENTITY AND CLOUD COMPROMISE

Mobile devices sit at the intersection of identity, communication, and cloud access. They host authenticator apps, certificate-based credentials, email, collaboration tools and business apps.

Identity Compromise
Attackers are shifting toward mobile identity theft. Session hijacking, MFA fatigue/AiTM attacks, and spyware allow adversaries to access cloud accounts even when MFA is enforced. The Paragon spyware case showed how silent mobile compromise provides direct access to sensitive data and communications.

Cloud Escalation
Verizon's Mobile Security Index (2024) notes that mobile compromise increasingly serves as a "cloud intrusion accelerator". Once an adversary steals mobile tokens or credentials, they pivot into SaaS platforms, email, storage, or VPN gateways.

Operational Impact
In organisations where staff rely heavily on smartphones/tablets (e.g., field units, critical infrastructure, emergency services), a compromised device can disrupt day-to-day operations or expose regulated data.

Mobile risk is enterprise risk. A compromised phone is often equivalent to a compromised identity, and therefore a compromised organisation.

A LAYERED APPROACH WITH MDM + MTD AT THE CORE

Recent assessments indicate that a Mobile Device Management (MDM) system alone mitigates up to 40% of mobile attack techniques. When combined with Mobile Threat Defence (MTD), coverage can increase to approximately 90%.

Sopra Steria has observed similar trends through its work in large-scale mobile fleet management and global deployments.

This gap exists because MDM manages devices but does not detect threats. MDM enforces configuration, inventory, and compliance – but cannot analyse network traffic, detect malicious apps, block phishing, or identify exploits.

MTD fills these gaps by providing continuous prevention, detection and remediation across all four vectors:

Prevent
Block malicious URLs, stop unsafe Wi-Fi, detect malicious certificates, prevent installation of high-risk apps.

Detect
Identify spyware, trojans, malicious SDKs, exploit attempts, jailbreak/root events, anomalous network behaviour, risky configurations.

Remediate
Integrate with MDM/UEM to quarantine devices, enforce updates, revoke tokens/certificates, or restrict access until risk is resolved.

This MDM + MTD interplay is essential for modern cloud and identity security.

SOPRA STERIA'S RECOMMENDED ACTIONS

01 **Strengthen Mobile Identity**
Implement phishing-resistant MFA (FIDO2, certificate-based), integrate mobile risk signals into conditional access, and monitor for AiTM or session hijacking.

02 **Ensure Mobile Hygiene & Baseline Security**
Mandatory patching, secure configurations, screen-lock policies, encrypted storage, disabled sideloading/USB debugging, and detection of jailbreaking/rooting.

03 **Integrate Mobile Telemetry Into SOC/IR**
Mobile threat alerts must feed into SIEM/SOAR pipelines, following the same workflows as traditional endpoint alerts. Adopt MITRE ATT&CK Mobile as a mapping framework.

04 **User Awareness for Mobile**
Train users on smishing, messaging-app link risks, QR-code attacks, rogue Wi-Fi, app permissions and reporting suspicious behaviour.

05 **Secure The Mobile Application Ecosystem**
Audit SDKs, permissions and supply-chain components, monitor for malicious updates, and enforce least-privilege principles for mobile apps.

05. CRITICAL INFRASTRUCTURE AND OPERATIONAL TECHNOLOGY

The long-held belief that Operational Technology (OT) was safe behind a wall of complexity is now dangerously obsolete. What was once a niche engineering field, shielded by "security by obscurity", is now a high-value target. Unlike IT systems, OT environments were never designed with cybersecurity in mind. They were built for reliability, longevity, and predictability. Their core function is to perform a single, deterministic task in a controlled environment, often utilising legacy systems that can't easily be patched or monitored. This makes them inherently vulnerable once connected to broader networks, creating an open door for modern threat actors. This exposure has turned these systems into an attractive target.

Three powerful forces are driving this shift: escalating geopolitical tension, business models demanding real-time operational data, and the rapid digitalization of critical infrastructure.

Sopra Steria has observed that there has been a significant rise in threats impacting industrial systems over the last few years, mostly due to geopolitical reasons. In 2024, 76 publicly reported incidents resulted in physical impact. Of these attacks, nearly 90% were indirect, meaning that the industrial systems themselves were not the primary target, but the attack successfully disrupted the underlying IT systems it relies on. However, the remaining 10% were direct targeted attacks that successfully shut down industrial operations.[5].

What we can learn from these attacks is the changing profile of the threat actors. The threat is no longer limited to sophisticated state actors, but is now dominated by geopolitically motivated hacktivists, often claiming to act in support of state operations. These groups are deliberately targeting industrial systems, yet their tactics remain largely opportunistic in nature. They seek out easily accessible targets and use low-skilled means, not complex exploits, to achieve their goal: defacement and disruption[6].

This shift has also been observed in Norway during 2025. Russia-affiliated hacktivist group gained access to the control panel of a water dam in Bremanger by exploiting a weak password, fully opening the outlet in an act of deliberate disruption. This so-called attack underscores a larger problem: industrial equipment often lacks necessary built-in security mechanisms to defend against modern threats, yet they are too often directly exposed to the internet[7].

This exposure is not purely a technical flaw, but also a human and organisational one. Engineering teams, focused on reliability and uptime, often establish connections without fully understanding the associated cyber risks. Many lack the digital maturity or cross-domain expertise needed to design secure, segmented architectures. At the same time, IT departments lack the fundamental understanding of industrial systems and are therefore reluctant to mandate or propose solutions that meet operational requirements.

[5] OT Cyber Threat Report – ICS Strive/Waterfall, 2025, https://icsstrive.com/wp-content/uploads/2025/03/2025-OT-Cyber-Security-Threat-Report.pdf
[6] It's time to act – National Cyber Security Centre, 2025, https://www.ncsc.gov.uk/files/ncsc-annual-review-2025.pdf
[7] https://www.nrk.no/vestland/pst-mener-prorussisk-hackergruppe-stod-bak-dam-sabotasje-pa-vestlandet-og-datainnbrudd-pa-ostlandet-1.17587446

At the core of this convergence challenge is a fundamental disconnect: engineering teams introduce exposures, while IT departments lack the operational context to effectively secure them. This highlights a critical point. The organisational silos of between IT and operational departments must be broken down. Not only is this best practice, but also a legal requirement under regulations like the digital security act (NIS2), which demands a unified risk approach.

An example of a threat emerging from this convergence is the unintended consequence of the green shift. The energy grid is becoming increasingly distributed and volatile, relying on renewable sources like solar panels, wind turbines, and battery storage. These systems are not like traditional, centralised power plants where four concrete walls protect and isolate the critical systems. They are complex ecosystems of IT and OT, fundamentally dependent on real-time communication, often over public networks, to control and balance the grid. This complex architecture does not easily fit with standard security practices and creates a large and hybrid attack surface.

> " Engineering teams introduce exposures, while IT departments lack the operational context to effectively secure them.

Adversaries are already taking notice. Groups ranging from advanced threat actors to hacktivists are actively targeting these systems[8]. However, the risk profile mirrors what we see in the broader threat landscape: the primary threat may not be a complex, direct attack on an OT component. Given the grid's dependency on dataflow and interconnectivity, it is equally vulnerable to indirect attacks. Relatively simple attacks, such as DDoS on public communication carriers or an attack on a central IT system, could disrupt the dataflow and following destabilising the grid. The uttermost consequence of such destabilisation being something similar of what we saw in Spain. Although that event was not the result of a cyberattack, it vividly illustrates the kind of nationwide blackout a targeted cyber operation against critical infrastructure could trigger.

FROM TECHNICAL PROBLEMS TO BUSINESS LIABILITY

While the industry often fixates on high-end, destructive scenarios like Stuxnet, BlackEnergy, and Triton, the immediate reality is simpler. The Bremanger dam incident was achieved with a weak password, demonstrating that the barrier to causing physical impact is low. The primary threat is not defined by its sophistication, but by its operational consequences.

The main threat vector is the dependency on IT systems. Incidents starting in traditional IT environments are proving to be effective in paralysing physical operations. Digitalisation creates a deep reliance on third-party vendors, remote access, and interconnected components, all of which expand the attack surface far beyond the organisation's direct control.

This expanded risk profile is no longer just a technical debate. Regulatory pressure, such as the Digital Security Act, legally mandates an integrated, holistic risk management approach. Regulators are explicitly demanding that organisations break down the silos of IT and OT security.

[8] DERs & Microgrids at Risk: How Adversaries Exploit Distributed Energy, 2025, https://www.dragos.com/blog/ders-microgrids-at-risk-how-adversaries-exploit-distributed-energy

THREAT VS. SYSTEM STRUCTURE

Because IT/OT systems used by critical infrastructure operators vary widely in structure, analysing threats in relation to system architecture is essential for prioritising security strategies. To support this, Sopra Steria has identified seven key types of critical infrastructure, outlining their core functions, system characteristics, and the most prominent threat category for each.

Energy Transmission and Management

Primary function of IT/OT:
Managing energy production/generation, transmission and distribution

Geographical distribution:
Wide

Volume of data in transit:
Moderate

Degree of interconnection:
Moderate

IT/OT characteristics:
- OT at key nodes
- Wide IT network connecting sites

Dependency on ISP/Telecom for communication:
High or Proprietary coms / lines

Most Prominent threat category:
OT Intrusions & Manipulation

Transport and Logistics Control

Primary function of IT/OT:
- Controlling physical transport infrastructure
- Controlling movement of rolling stock/transport fleet
- Controlling key equipment at important nodes

Geographical distribution:
Wide

Volume of data in transit:
Moderate

Degree of interconnection:
Moderate

IT/OT characteristics:
- Small OT elements at high number of sites
- OT/ IT elements in moving stocks/cars
- Wide IT network connecting

Dependency on ISP/Telecom for communication:
High or Proprietary coms /lines

Most Prominent threat category:
OT Intrusions & Manipulation

Surveillance

Primary function of IT/OT:
- Air traffic control
- Military surveillance of air and sea territory

Geographical distribution:
Wide

Volume of data in transit:
Moderate

Degree of interconnection:
Limited or separated

IT/OT characteristics:
- OT controlling sensors
- Wide IT network connecting sensors

Dependency on ISP/Telecom for communication:
High or Proprietary coms / lines infrastructure

Most Prominent threat category:
- OT Intrusion & Manipulation
- Espionage

Telecommunication Networks and Datacentres

Primary function of IT/OT:
- Tele/data communication
- Data processing and storage

Geographical distribution:
Wide

Volume of data in transit:
Very High

Degree of interconnection:
Very High

IT/OT characteristics:
IT-networks (including large volumes nodes and centres)

Most Prominent threat category:
- Extortion Against IT Systems
- Espionage

Digital Networks for Governmental and Societal Functions

Primary function of IT/OT:
- Governing
- Financial operations
- Protection of society (police, military or courts)
- Managing the census
- Managing health and social services

Geographical distribution:
Wide or Local (Varies by system)

Volume of data in transit:
Moderate to high (Varies by system)

Degree of interconnection:
High

IT/OT characteristics:
IT-systems

Most Prominent threat category:
- Extortion Against IT Systems
- Espionage

Larger Industrial Production Chains

Primary function of IT/OT:
Industrial production

Geographical distribution:
Local or Limited number of sites

Volume of data in transit:
Low

Degree of interconnection:
Limited

IT/OT characteristics:
- OT-systems
- Local IT networks connecting
- IT management systems

Most Prominent threat category:
- OT Intrusions & Manipulation
- Espionage

Provision of Physical Public Utilities

Primary function of IT/OT:
Water, sewage

Geographical distribution:
Local

Volume of data in transit:
Low

Degree of interconnection:
Limited

IT/OT characteristics:
- OT-systems
- Local IT networks connecting

Most Prominent threat category:
OT Intrusion & Manipulation

SOPRA STERIA'S RECOMMENDED ACTIONS

The path forward requires a shift in perspective. Effectively managing this threat landscape and following risks depends on two key actions: achieving greater operational visibility into these converged environments and fostering a collaborative security culture between IT and OT teams.

Focus On The Value Chain, Not The Asset
A complete asset inventory is the foundation, but it is not the end goal. The priority should be to map the critical value chains, the end-to-end processes that deliver the service to the end-user, such as drinking water to the citizens. This allows for security efforts to be focused on protecting the most critical functions from downtime, whether the threat originates in IT or OT.

Build a Resilient and Defensible Architecture
The primary threat is disruption via IT systems and networks, which is increasingly interconnected to OT. This requires resilient architecture, minimising the attack surface, and crucially implementing converged monitoring. Gaining unified visibility across all IT and OT networks is the only way to detect the spillover and indirect attacks that cause the most damage.

Adopt Zero Trust Segmentation
The "air gap" is a myth, containment is the imperative. A zero-trust model is the technical implementation of resilient architecture. By enforcing micro segmentation, not just between IT and OT, but within the industrial environment itself, breaches can be contained and prevent them from paralysing all physical operations.

06.
REGULATORY AND **LEGAL LANDSCAPE**

Sopra Steria are observing how new security regulations are adopted at an ever increasing pace. In 2025, the Norwegian Parliament adopted several laws that directly or indirectly affect cybersecurity, the most important being the Norwegian Digital Security Act (NIS1) and the Digital Operational Resilience Act (DORA). In addition, the Artificial Intelligence Act (AI Act), which has been circulated for public consultation, is expected to be adopted into national law in 2026.

All of these frameworks highlight resilience; the ability to ensure continuity of an organisation's critical services in the event of a cyber incident. Customers (both public and private) increasingly require suppliers and partners to demonstrate sound security governance. For many organisations, the ability to maintain cybersecurity has become a prerequisite for participating in the market. Organisations that fail to take this development seriously risk losing trust, customers, and market shares.

Another trend we see is that responsibility is increasingly directed towards top management. Regulations now establish that cybersecurity is part of overall corporate governance, and that boards and senior executives must have sufficient understanding of cyber risks to make informed decisions. The Norwegian Digital Security Act is a clear example: it requires management to approve security measures, monitor compliance, and may hold members of management bodies personally liable in the event of non-compliance. The same pattern can be seen in DORA for the financial sector and in the AI Act, where requirements for risk management and oversight of technology use are placed at the management level.

Third-party management has also become a central focus. New regulations recognise that an organisation's security is heavily influenced by its suppliers, partners, and subcontractors. This extends beyond technical deliveries to include consultants, system operations, data processing, and cloud services. Organisations are no longer responsible only for their own systems but also for security across the value chain. In our opinion, this should translate into new expectations for contracts, control procedures, and ongoing follow-up.

CYBER RISK HAS YOUR NAME ON IT

Legal risk itself is also changing in nature and scope. Where it once centred on contracts, compliance, and disputes, it now extends across the organisation's entire digital operations. Cybersecurity, data protection, artificial intelligence, sustainability, and third-party management are all areas where new regulatory frameworks intersect and reinforce one another. This means that legal risk can no longer be managed in isolation – it requires close cooperation between legal, technical, and executive functions to ensure that decisions are both compliant and strategically sound.

For leaders, this represents a fundamental shift in responsibility and expectations. Whereas it was once possible to delegate security to the IT department, it is now expected that leadership itself has a conscious understanding of risks, vulnerabilities, and consequences. The regulatory frameworks assume that security work is integrated into the organisation's overall governance system – on par with financial management and quality assurance.

> "Under The Norwegian Digital Security Act, individuals can face personal economic responsibility up to 25 times The Norwegian Social Insurance Scheme's basic amount (3 254 000 NOK as of 2025).

It is expected that more future regulatory frameworkds will introduce sanctions that may apply not only to the organisation, but individual members of managements bodies. This will typically be the body responsible for developing the company's strategy and overall objectives and for monitoring management's decisions, usually the board of directors. Under The Norwegian Digital Security Act individuals can face personal economic responsibility up to 25 times The Norwegian Social Insurance Scheme's basic amount (3 254 000 NOK as of 2025).

This reflects a trend towards more individualised accountability, highlighting how regulatory frameworks potentially can hold top management directly responsible, using personal sanctions to reinforce that accountability cannot simply be delegated.

At the same time, management is expected to have sufficient competence to understand and follow up on security risks. Additionally, the legal responsibility to control and follow up on third parties is becoming both broader and more complex. For management, this means that security governance must become more systematic, documented, and risk-based. Having technical measures in place is no longer sufficient, it must be possible to demonstrate how these measures align with organisational goals, risk assessments, and decision-making processes.

SOPRA STERIA'S RECOMMENDED ACTIONS

To meet the legal and strategic changes ahead, Sopra Steria recommend that organisations strengthen their cybersecurity governance systems and risk management processes. The first step is to establish clear lines of responsibility. Boards and senior management should explicitly define who is responsible for following up on security efforts and how this is reported. Clear accountability contributes both to compliance and to better decision-making.

Management should also ensure that their competence level is sufficient to understand and assess cybersecurity risks. This does not mean that all leaders must be technical experts, but they must understand how security affects operations, values, and reputation. Many organisations are now establishing dedicated training programmes for boards and executives in this area.

Another key area is supply chain management. Sopra Steria recommends that organisations identify which third-party relationships are critical to operations and security, and establish routines for assessment, contracting, and follow-up. The requirements in the Digital Security Act and DORA make this a leadership responsibility. A central principle is that responsibility cannot be outsourced – the organisation remains accountable for security even when services are provided by others.

Documentation and incident reporting have also become central elements of security governance, and are central duties under both DORA and the Digital Security Act, with multiple tight deadlines for reporting to authorities. Many regulatory frameworks require organisations to document how risks are assessed, how measures are decided, and how incidents are handled. This demands strong routines and a governance system that is more than a formal process – it must be a dynamic tool that supports organisational decision-making.

Finally, it is important to highlight the need to view cybersecurity in connection with the organisation's overall business strategy. Increasing digitalisation and the use of artificial intelligence, cloud services, and data sharing mean that security can no longer be treated in isolation. It is an integrated part of innovation, efficiency, and value creation. For management, the task is therefore not only to reduce risk but to ensure sustainable and trust-based development.

07. **GOVERNANCE, RISK, AND COMPLIANCE:** A STRATEGIC IMPERATIVE

> "Organisations have more data than ever, but lack actionable insight.

In 2026, cybersecurity is more complex than ever. Digital transformation, regulatory pressure, and evolving threats have made one thing clear: Fragmented approaches to governance, risk, and compliance (GRC) are no longer viable. Sopra Steria believes resilience requires holistic digital governance; a unified approach that embeds cybersecurity into enterprise management.

FROM COMPLEXITY TO COHERENCE

Despite years of investment, many organisations still govern in the dark. Governance, risk, and compliance often run on parallel tracks, and they are disconnected from strategy and operations. Without integrated tooling, visibility, and proactive decision-making is nearly impossible.

This fragmentation is not just inefficient – it's risky. Legacy models cannot handle today's complexity, leaving leaders with outdated structures and limited insight. GRC maturity is often low, incoherent, and misaligned – unfit for the digital age. Sopra Steria emphasises that a strategic shift towards holistic, proactive security management is imperative. This should be driven by regulatory change, complex threats, and expanding attack surfaces.

WHY THIS MATTERS NOW

Pressure Is Mounting

Regulatory Complexity
NIS2, DORA, AI Act demand integrated oversight.

Supply Chain Risk
54% of security leaders identify lack of visibility as a top concern.

Sophisticated Threats
Attacks now target trust, not just systems.

Stakeholder Expectations
Transparency and ethical tech use are non-negotiable.

Resource Constraints
Leaders must do more with less.

Governance is no longer a back-office function. It is a strategic capability for aligning decisions with risk appetite, enabling responsible innovation, and protecting long-term value. With 72% of security leaders reporting increased cyber risk – and AI adding complexity – a shift in both proactive and reactive approaches is critical.

THE INFORMATION PARADOX

- Organisations have more data than ever but lack actionable insight.
- 67% of compliance leaders want better data quality for risk detection.[9]
- 64% seek better measurement of compliance effectiveness.[9]
- Only 23% feel confident managing governance amid AI and regulatory change.[10]

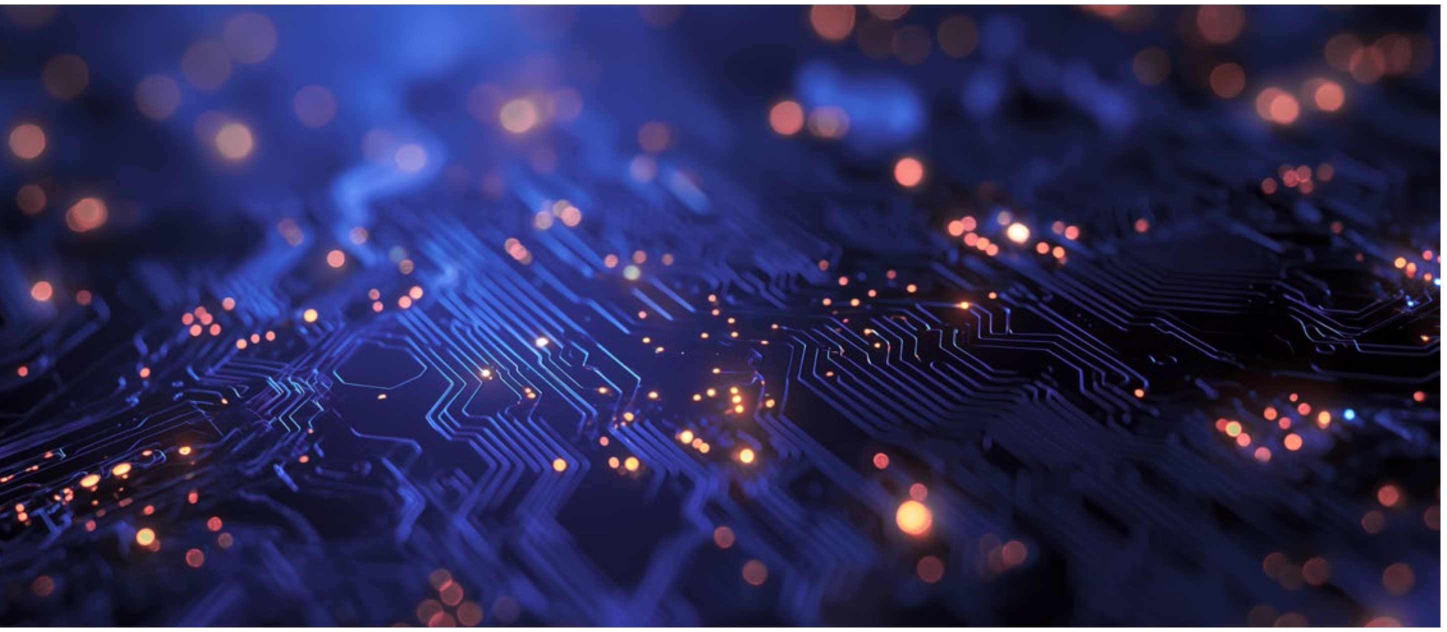
Static, reactive governance cannot keep pace with digital transformation. Sopra Steria has seen how this creates critical challenges, especially for medium and large enterprises, where complexity makes relevant security decisions difficult. The result is a widening gap between what leaders need to know and what their systems can tell them.

WHAT NEEDS TO CHANGE

Based on Sopra Steria's experience and best practice, closing the governance gap means:

- Treat governance as leadership, not administration.
- Break silos between risk, compliance, IT, and business.
- Shift from periodic reporting to continuous insight using real-time data and predictive analytics.
- Embed governance into operations, not bolt it on.
- Recognise digital risk as business risk.

This is how cybersecurity, risk and compliance can be turned into actionable insight for top management.



MAKING RISK REAL: QUANTIFICATION

One of the most persistent challenges in cybersecurity is relevance. While technicians speak in vulnerabilities, threat vectors and patch cycles, executives think in financial impact, business continuity and strategy. Bridging the gap requires more than dashboards – it requires quantification.

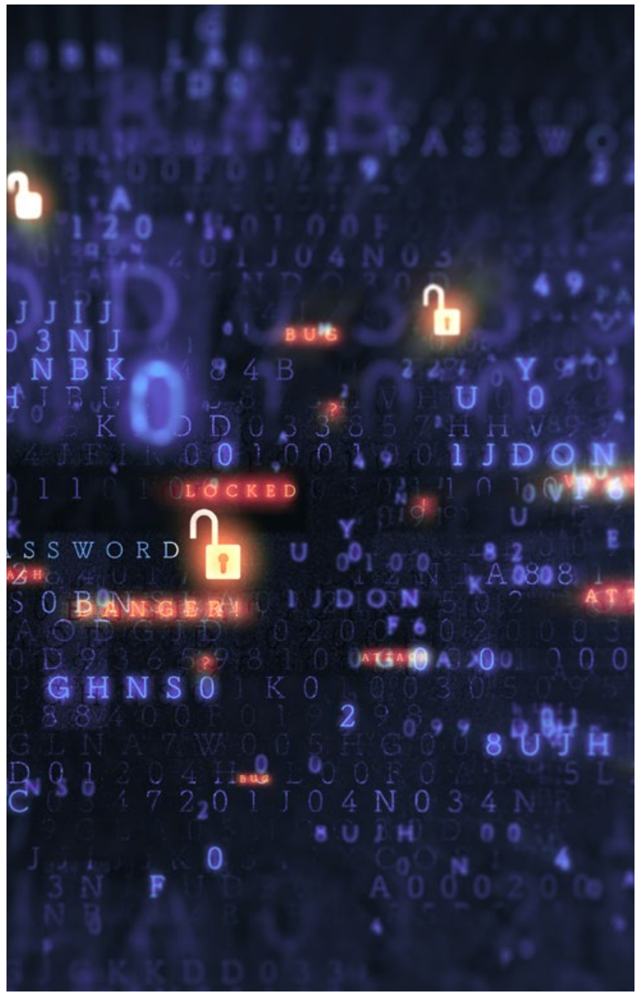
Quantifying risk and compliance in financial terms increases the relevance of this important decision making tool, and provides valuable input to financial processes as well as business cases for improvement initiatives or investments: Calculating Annual Loss Expectancy (ALE) and cost of mitigation translates risk into monetary terms and enables cost-benefit analysis, prioritization, and strategic alignment.

Quantifying Also Means Using Data To

- Estimating the probability of a risk event (based on empirical data or predictive models)
- Assessing the potential impact (based on historical losses or scenario analysis)
- Combining the two to derive a quantified risk exposure

This approach answers key questions: What is the cost of inaction? Where should we invest? Which risks are acceptable?

In Sopra Steria's view, this method helps modern governance be relevant, proactive, and cost-effective.



DATA-DRIVEN EFFICIENCY

Modern governance must automate detection, prioritisation, and compliance monitoring. Data should be used not just for reporting, but for driving automated detection, prioritization, and response. Predictive analytics and artificial intelligence are increasingly expected to identify patterns and estimate likelihoods. Sopra Steria recommends this approach because automation and intelligence are key to reducing complexity, accelerating decision-making, and ensuring resilience in a rapidly evolving threat landscape.

[9] 2026 Strategic Priorities for Chief Compliance Officers | Gartner
[10] Gartner Predicts AI Regulatory Violations Will Result in a 30% Increase in Legal Disputes for Tech Companies by 2028

FROM INSIGHT TO IMPACT

All in all: It's about making empirical, analytically sound, risk-based decisions. With the right skills and experience, this is far from utopia – it's a practical way to elevate the CISO's voice and position of cybersecurity as a true strategic capability.

Effective Governance Delivers

Strategic Alignment
Risks tied to business goals.

Efficiency
Automation replaces manual reporting.

Resilience
Anticipate change, avoid crises.

Trust
Transparency builds confidence.

Innovation
Clear guardrails enable faster progress

Let your security experts simplify complexity. GRC teams should move beyond static documents to become operational partners – using technology to connect data, automate assessments, and push dynamic requirements.
This approach cuts through manual processes, reduces disruption, and ensures that risk and compliance enables actionable governance across the business.

A WORD OF CAUTION

There is no silver bullet. Implementing holistic digital governance is not about buying a platform or adopting a framework. It's about changing how decisions are made, how information flows, and how accountability is shared. It requires leadership, cultural change, and sustained effort.

Succeeding will enable organisations to regain the trust they currently lack – trust eroded by the gap between abundant data and truly actionable information.

SOPRA STERIA'S RECOMMENDED ACTIONS

Adopt Holistic Digital Governance
Move from fragmented GRC practices to an integrated, enterprise-wide approach that embeds cybersecurity into business strategy and operations.

Treat Governance as Leadership, Not Administration
Position GRC as a strategic capability for aligning decisions with risk appetite and enabling responsible innovation.

Break Down Silos
Integrate risk, compliance, IT, and business functions to ensure coherence and visibility.

Shift to Continuous Insight
Replace periodic reporting with real-time data, predictive analytics, and proactive decision-making.

Embed Governance Into Operations
Make GRC part of everyday processes rather than an add-on activity.

Recognise Digital Risk as Business Risk
Elevate cybersecurity and compliance to the same level as financial and operational risks.

Quantify Risk in Financial Terms
Use methods like calculation of Annual Loss Expectancy (ALE) and cost-benefit analysis to translate technical risk into business-relevant language.

Leverage Data-driven Efficiency
Automate detection, prioritisation, and compliance monitoring the organization's data, and preferably using AI and predictive analytics.

Enable Strategic Alignment and Resilience
Tie risks to business goals, anticipate change, and avoid crises through proactive governance.

Empower GRC Teams as Operational Partners
Move beyond static documentation to dynamic, tech-enabled processes that simplify complexity and reduce disruption.

Focus on Cultural and Leadership Change
Understand that success requires more than tools – it demands new decision-making models, accountability, and sustained effort.

08. **PEN TESTER'S** INSIGHTS

> "Attackers don't need new tricks when the old ones still work perfectly well.

Over the past year, Sopra Steria Scandinavia's penetration testing team has continued to see the same core weaknesses across organisations of all sizes and sectors. These are not new or advanced vulnerabilities, but long-known issues that persist because of operational complexity, legacy systems, and gaps in governance. They still give attackers reliable ways to escalate privileges, move laterally, and compromise critical systems. Addressing these recurring weaknesses is key to reducing risk, and meeting the growing expectations set by today's regulatory and resilience frameworks.

Active Directory (AD) continues to play a central role in identity and access management, even as more workloads move to the cloud. Many environments now run hybrid identity setups, where on-premises AD integrates with Azure AD or other cloud platforms. This hybrid model still exposes many of the same traditional AD weaknesses that attackers can exploit to gain privileged access.

From Sopra Steria's penetration tests over the past year, we continue to observe the following recurring issues:

- Weak password hygiene, including short passwords based on company names, seasons, years, or personal names. We also continue to see the same passwords reused across multiple accounts, including service and administrative accounts, and admin passwords that haven't been rotated for long periods.
- Credentials stored in file shares or configuration files. These exposed secrets often give direct access to business-critical systems.
- Legacy Windows protocols can enable attackers to intercept credentials on the network and reuse them to authenticate elsewhere. Attacks, such as credential relaying, remain effective in environments where these older protocols are still enabled and signing is not enforced.
- Misconfigured AD permissions and certificate services, where overly permissive rights or weak certificate templates allow attackers to escalate to domain-administrator level.
- IT management platforms (e.g. SCCM) can be abused by attackers to move laterally or deploy malicious code at scale.
- A lack of administrative tiering, with privileged accounts reused across workstations, servers, and domain controllers, allows a single compromise to escalate quickly into a full domain takeover.

These findings confirm that identity infrastructure remains one of the most common entry points for compromise.

Weaknesses in AD and hybrid identity environments continue to give attackers a reliable way to move from initial access to full control. For many organisations, AD remains deeply embedded in business-critical operations, and the security of that foundation directly affects resilience, regulatory compliance, and incident response capability.

New legislation such as the EU's DORA regulation and the Digital Security Act now set explicit requirements for operational resilience, identity protection, and regular security testing. Compliance to this is no longer optional, but a legal obligation.

SOPRA STERIA'S RECOMMENDED ACTIONS

Strengthen Authentication Controls
Make authentication a core focus. Use longer passwords in line with CISA recommendations. Require passwords to be at least 15 characters in length to improve resistance to brute-force, and password-guessing attacks. Always require multi-factor authentication for key systems. Even if an attacker manages to obtain a user's password, MFA makes it significantly more difficult for them to access sensitive systems, as they would also need the second factor. Where possible, choose phishing-resistant MFA methods, such as FIDO2 security keys to further reduce the risk of compromise from phishing attacks. LAPS Should always be used to ensure each system has a unique, automatically rotated local administrator password, and migrate service accounts to Group Managed Service Accounts (gMSA) where possible to remove static credentials.

Protect Sensitive Data
Audit shared storage, configuration files, and code repositories on a regular basis to identify any exposed credentials. Move secrets to a secure, centralised vault, and make secret management part of normal development and operational routines.

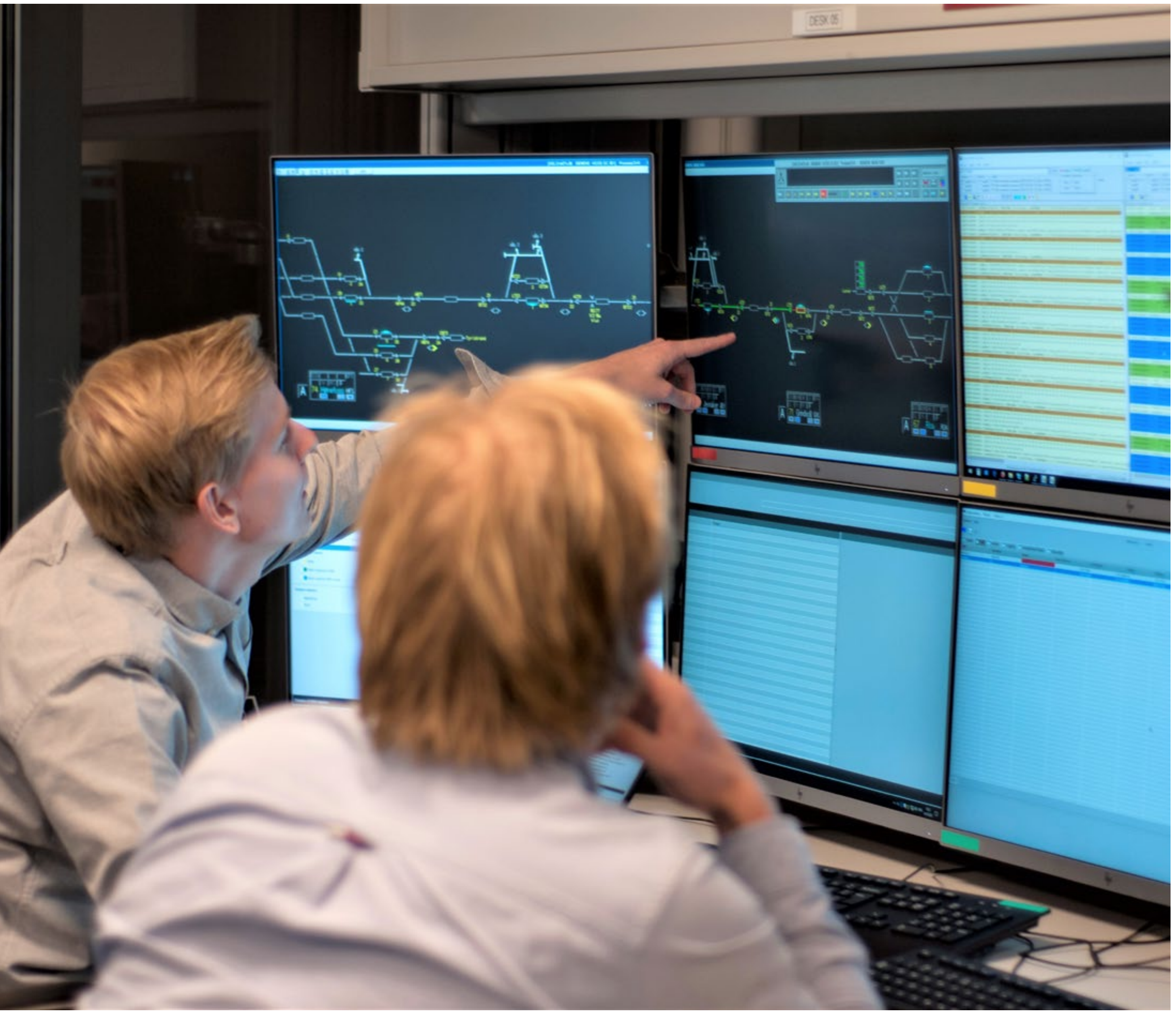
Harden Configurations
Treat configuration hardening as an ongoing discipline, not a one-off task. Retire older network protocols that no longer serve a purpose, and make sure SMB and LDAP signing are consistently enforced. Periodic reviews of certificate templates and directory permissions help remove unnecessary privileges, and reduce the risk of escalation if an account is compromised.

Implement Administrative Tiering
Use separate administrative accounts for different levels of access, such as workstations, servers, and domain controllers. Applying this model consistently limits how far an attacker can move if one credential is compromised.

Adopt Continuous Security Testing
Move beyond traditional, point-in-time penetration tests. Continuous testing helps uncover new weaknesses and configuration drift as they appear, giving earlier visibility and faster remediation.

These measures not only reduce the likelihood of compromise but also demonstrate compliance with emerging regulatory expectations across Europe and the Nordics.

> "New legislation set explicit requirements for operational resilience, identity protection, and regular security testing. Compliance to this is no longer optional, but a legal obligation.



09.
CUSTOMER'S STORY

BANE NOR

> "The key is building and providing modern digital services that effectively support key business processes and users to work effectively, delivering core functions and timely relevant information to society. These critical operational functions needs to be resilient and defendable over time to ensure continuous and trustworthy services.

Tom Remberg // CISO Bane NOR

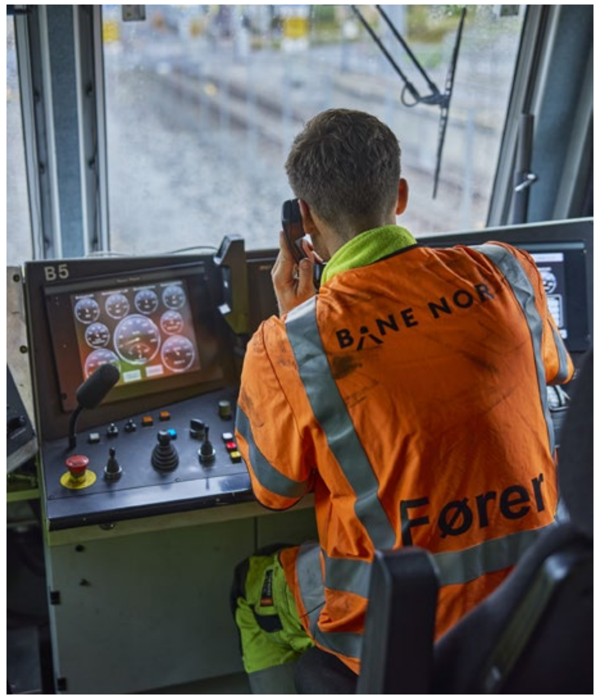
Bane NOR plays a critical role in Norway's national security and emergency preparedness. Railway transport is defined as a fundamental national function, responsible for safety, accessibility, and maintaining the critical transport infrastructure.

In times of crisis, the railway is essential for moving key personnel, sustaining the flow of goods, and ensuring access to vital raw materials – including international supply chains. It also provides the capability to transport large volumes of heavy military equipment over long distances. With Sweden and Finland joining NATO, the strategic importance of the railway for Norway has become even more pronounced.

Under normal circumstances, Bane NOR serves as Norway's railway infrastructure manager, developing, building, operating, and maintaining the national railway network. In addition, Bane NOR manages train traffic and railway property, enabling more people to travel by train – a green and sustainable solution for both freight and passengers.

The Norwegian railway is undergoing a comprehensive modernization to integrate advanced technologies and improve operational efficiency. Key development projects, maintenance, renewal, digitalization, data-driven insights, efficient data flow, and new technologies are central to delivering a safe and accessible railway infrastructure. In integrating new technologies, automation and IT development also play a central role. Digital security is not only about protecting against malicious activity; the effective use of modern security solutions also serves as a critical business enabler. This exciting transformation allows digital security to have a central place throughout the organisation.

Digitalization offers significant opportunities to streamline operations and services, but it also increases exposure to new types of cyber threats. The global security landscape affects Bane NOR's threat landscape. A clear trend is observed: critical business functions are increasingly dependent on digital systems. In Europe and the Nordic region, incidents targeting the transport and railway sectors have increased in recent years. It is expected that this trend will continue, and one must be prepared for the possibility that the Norwegian railway could also be affected.



Heightened digital vigilance must become an integral part of daily operations. Bane NOR will continue working in a structured, strategic, and targeted manner, integrating security by exploring and adopting modern digital solutions to support digitalization.

BANE NOR'S DEFENDABLE OPERATION PROGRAM

Strengthening Bane NOR's ability to defend, secure, and consistently deliver robust critical functions – both in normal operations and during crisis – is essential. To achieve this, Bane NOR has launched a major strategic improvement initiative: The Defendable Operation program. Its goal is to ensure Bane NOR can deliver critical business services even under advanced, prolonged, and destructive cyberattacks.

Building a digitally resilient society requires acknowledging our dependence on digital solutions. This demands commitment, competence, and close collaboration among all stakeholders who play a role in securing a robust digital Norway.

EMBEDDING SECURITY INTO DAILY IT OPERATIONS

Defendability starts with strong IT hygiene and a secure operational IT infrastructure. These fundamentals are essential for enabling Bane NOR's critical business functions and achieving the objectives of the Defendable Operation program. Without a solid, secure foundation, Bane NOR cannot ensure the resilience required to deliver safe and reliable railway services.

Sopra Steria plays a strategic role in this journey, serving as both Managed Service Provider (MSP) and Managed Security Service Provider (MSSP) for Bane NOR's enterprise business IT infrastructure, operating as a dedicated SOC to ensure protection 24/7, 365 days a year. This means working proactively to reduce the attack surface, safeguard critical business services, protect identity, and enhance monitoring and response capabilities so that anomalies can be detected and handled quickly.

These initiatives, combined with the Defendable Operation program, demonstrate Bane NOR's commitment in strengthening its digital infrastructure, ensuring resilience against a dynamic threat landscape, and sustaining a robust foundation to achieve its core business objectives – while focusing on risk-driven improvement efforts.

> "When embarking on a digital resilience and defendable journey, make sure to keep the business perspective and rationale at the forefront. Furthermore, make clear priorities within the program, focusing on critical business functions. Identify what matters most to the business and make that your starting point.
>
> *Tom Remberg // CISO Bane NOR*

10.
OUTLOOK
2026

> " AI accelerates everything; attack tempo, defensive capability, and the need for AI-specific governance and safeguards.

As we enter 2026, cybersecurity is shaped by two dominant forces: accelerating technological change (especially AI), and intensifying geopolitical tension. Together, they increase operational risk, expand the attack surface, and push organisations toward more rigorous resilience, governance, and verification models.

ARTIFICIAL INTELLIGENCE

AI will significantly amplify both attack and defense:

Offensive Use Grows
Threat actors will use agentic AI to speed up malware development, automate exploitation, and support lateral movement. Realistic synthetic content will fuel more effective social engineering, fraud, and disinformation.

Defensive Use Matures
AI-driven detection, analysis, and automated response will become core capabilities, acting as a force multiplier for defenders.

The overall effect: AI accelerates everything; attack tempo, defensive capability, and the need for AI-specific governance and safeguards.

GOVERNANCE, RISK & COMPLIANCE

2026 brings stricter accountability and more complex supply-chain exposure:

Supply Chain Risk Intensifies
Adversaries increasingly target third-party software, open-source components, and service providers.

Three EU Regulations Define The Compliance Landscape
NIS2, DORA, and the Cyber Resilience Act shift expectations from policies to evidence of resilience through testing, logging, patching processes, and third-party oversight.

Data Sovereignty Rises
The EU Data Act and ongoing scrutiny of extraterritorial access drive requirements for EU-only services, customer-managed keys, geo-fencing, and stronger contractual controls.

Organisations must combine technical safeguards with contractual discipline and continuous monitoring to maintain compliance.

THREAT LANDSCAPE

Threat actors in 2026 will focus on identity, supply chains, and high-impact infrastructure:

State-backed and Proxy Operations Increase,
combining espionage, pre-positioning, influence operations, and occasional disruptive activity—with growing focus on critical infrastructure and OT/ICS environments.

Identity Remains The Number-one Attack Surface
Expect more token/session theft, federation abuse, MFA-bypass kits, OAuth manipulation, and targeting of non-human identities such as service principals and API identities.

Self-compromise Attacks Rise
ClickFix, FileFix, Fake Update Scams, and deepfake-enabled tutorials grow as AI personalises and automates social engineering.

Software Supply Chain Attacks Expand
Attackers probe CI/CD pipelines, build systems, and code repositories; dependency hijacking, typo-squatting, and maintainer account takeovers continue to grow.

Overall, attackers will prioritise paths that scale: identity systems, managed service providers, cloud trust relationships, and CI/CD environments.

WHAT ORGANISATIONS NEED IN 2026

Despite growing complexity, the threat landscape remains manageable with the right foundations:

Zero Trust in Practice
Identity proofing, phishing-resistant MFA, least-privilege, JIT access, continuous device health checks.

Modern Detection & Response
Fusion of endpoint, identity, email, network, and cloud telemetry.

Strong Governance
Clear risk ownership, actionable metrics, tested response plans, compliance with NIS2 and DORA.

Back to Basics
IT hygiene, vulnerability reduction, asset visibility, and disciplined patching remain decisive.

The security model must evolve from “trust-but-verify” to continuous “verify-then-trust.” With deepfakes, AI-driven identity abuse, and supply-chain compromise on the rise, organisations can no longer assume authenticity. Every person, system, and signal must be validated.

> “Organisations can no longer assume authenticity. Every person, system, and signal must be validated.

11. **FINAL** NOTES

The trends show a threat landscape that is accelerating together with AI. But even if AI is the big hype, and on everyone's agenda, we cannot emphasise enough the work that needs to be done on your basics. Most cyberattacks that affect the vast majority of companies succeed due to exploitation of missing basic IT-hygiene. This means that working systematically with reducing your external attack surface is one of the best investments you can make. Ensuring you have a well-functioning vulnerability management process in place, which makes it possible to rapidly patch or isolate critical systems when new vulnerabilities are known, is key.

> "If I had to describe the past year's changes in the threat landscape with one word, it would be this: Tempo. Everything is accelerating and the volume of attacks keeps rising; yet most successful breaches still stem from missing basic IT hygiene.

AI is for sure one of the disruptors in our industry, and we at Sopra Steria work hard to make sure it helps us in our defensive effort. But the shift toward AI technologies does not mean you should reduce your focus on implementing 'good old-fashioned IT best practices'.

Lifecycle management and infrastructure are key components in meeting the threats of tomorrow. Making sure your infrastructure is up to date is imperative if you want to do "all the cool stuff" like orchestration, automation, and having capabilities that enables the most critical assets to run in isolated mode when the attacks eventually happen.

Understanding your own threat landscape and following threat actors around the clock is important, but a very specialised competence and service. So make sure to partner up with a MSSP that can provide these kinds of services for you.

If I had to describe the past year's changes in the threat landscape with one word, it would be this: Tempo. Everything is accelerating, and the volume of attacks keeps increasing.

We hope you enjoyed this report and that it gives you valuable insights when prioritising your efforts moving into 2026 and beyond.

As always at Sopra Steria we are here to help. So, if you want a discussion, a sparring on your security strategy, or a look into what Sopra Steria can do to help you; please reach out.

Best regards,

Jørgen Rørvik
Director of Cybersecurity
Sopra Steria Scandinavia
e-mail: Jorgen.rorvik@soprasteria.com

STATE OF

CYBER SECURITY

2026

The world is how we shape it.

www.soprasteria.no