CYBERSECURITY IN NORWAY MARKET GROWTH

Radar.

JUNE 2025

DIFFERENT CYBERSECURITY STRENGTHS IN SWEDEN AND NORWAY

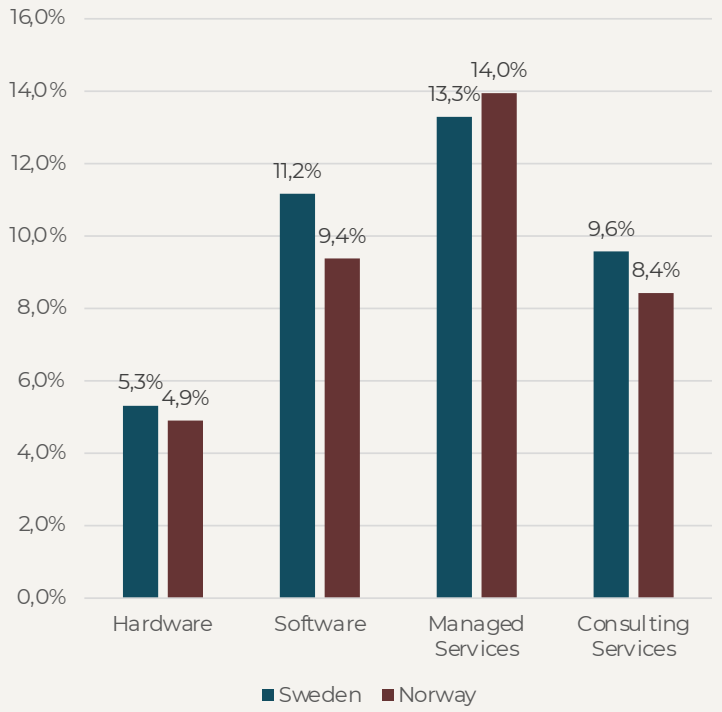
Hardware (firewalls, IDS/IPS, appliances)
Sweden has a more developed cybersecurity industry linked to the defense sector (e.g., SAAB, Combitech, etc) than Norway and f.ex. Kongsberg. Norway invests in critical infrastructure (oil, energy), but the scale of the hardware segment is in total slightly lower in growth.

Software (SIEM, IAM, EDR/XDR, etc.)
Sweden has more cybersecurity companies and faster adoption of certain advanced (more costly) security solutions (Zero Trust, SASE, etc.).
In Norway, large players dominate, but the SME segment is lagging.

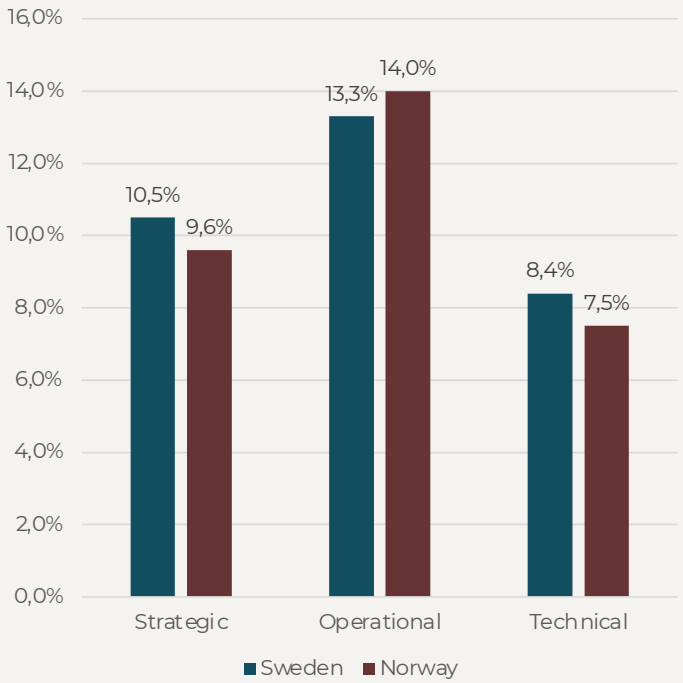
Managed Services
Many Norwegian organizations choose to outsource cybersecurity functions (e.g., SOC) to external vendors.
Strong players include everything between the likes of Mnemonic, Orange Cyberdefense, Advania Cyberdefence Center, Defendable, Atea, Netsecurity and Sopra Steria, to mention a few.

Consulting Services
Norway has strong in-house expertise, especially in regulated sectors (e.g. oil and energy). Advisory services related to Digital Security (implementation of NIS1) ,NIS2 and ISO 27001 increased sharply in 2023–2024, and coming regulations means the advisory services will continue to grow in 2025, though weaker growth than Sweden. This could be due to Sweden having coming NIS2 requirements, which will be in effect from January 2026.

MARKET GROWTH, 2025



MARKET GROWTH, 2025



STRATEGIC, OPERATIONAL, AND TECHNICAL PERSPECTIVES

Strategic (Policy development, compliance, risk management, CISO functions)
Expected NIS1 and coming NIS2 implementation drives the need for governance, but Norway already has high regulatory maturity in critical sectors, which reduces the growth potential somewhat.

The SME sector in Norway has fewer CISO roles per capita compared to Sweden, and a reliance on internal policy development over external advisory services, which may result in lower demand for cybersecurity consulting than comparable markets.

Operational (SOC, incident handling, MDR/XDR, processes & monitoring)
Operational services are growing rapidly through service providers (MDR, SIEM, SOC-as-a-Service) and crisis/cyber exercises (driven by campaigns from DigitalNorway, NSM, DNV, among others).The energy, transport, public sectors and other critical sectors are major buyers.

Technical (Hardware, software, implementation, technical controls)
Norway, like Sweden, prioritizes services rather than developing new technical platforms for its own implementation. This is still partly driven by ongoing investments in cloud security and EDR/XDR, though these efforts lack breadth, especially in areas such as on-premise firewalls and IAM systems.

OTHER DEVELOPMENTS AFFECTING THE CYBERSECURITY MARKET IN NORWAY

The EU's Digital Operational Resilience Directive, (DORA) aims ensure a high level of digital operational resilience among entities in the financial sector. DORA will be implemented in Norway July 1st.2025.

DORA provides rules for risk management, incident handling, testing of digital operational resilience, third-party risk management, and information sharing around ICT.

For other essential and critical sectors in Norway the coming NIS1- implementation in the form of Digital Security Act and coming NIS2 Directive will raise security standards and create a uniform legal framework for network and information systems.

The previous implementation of the NIS Directive is widely considered to have taken too long, and government has signaled that implementation of NIS2 will be swifter.

The Norwegian government has recently allocated millions in cybersecurity projects.

Further, well-established companies with strong reputations are actively expanding their cybersecurity initiatives. One recent example is Telenor, who establishes a new cybersecurity company with a SOC focusing on the Nordic market.

There is also a growing demand for cybersecurity consulting services in Norway, especially in areas such as network security, cloud security, and regulatory compliance (both current and upcoming).

Norwegian technology exports remain somewhat limited, especially when compared to Swedish cybersecurity firms.

The Norwegian Security Service (PST) has identified an increased risk of cyberattacks from state actors, increasing awareness and the need for robust cybersecurity measures.

Radar.

Radar supports all actors in the IT ecosystem in making informed decisions at the right time. Our data-driven insights and tools help you grow and succeed in your mission in the digital future.

By combining data and analysis with experience and methodology, we empower IT and tech suppliers and decision-makers to lead with data-driven insights.

With Radar's unique position as a trusted and independent party, we create value for the IT ecosystem by delivering reports and key metrics, digital tools, strategic advisory services, and events.

Find more information at https://radargrp.com