DNV CYBER

NORDIC CYBER RESILIENCE

HOW CYBER RESILIENT IS NORWAY?

Strengthening the resilience of Norway's critical infrastructure and society

ABOUT THIS RESEARCH

This report is part of a larger research project exploring the cyber resilience of critical infrastructure across four Nordic countries: Sweden, Finland, Norway, and Denmark. The project is being run by DNV Cyber, a leading cybersecurity services provider helping businesses become safer and more resilient in an increasingly complex risk landscape.

Focusing on Norway, the report includes three sources of information: a survey of 200 senior critical infrastructure executives in Norway, from industries including maritime, healthcare, energy, and public administration; a survey of 500 members of the public in Norway; and seven in-depth interviews with leaders and experts in the field of cybersecurity. The report was developed in partnership with FT Longitude (a Financial Times company). Research was conducted from November 2025 to January 2026.

ACKNOWLEDGEMENTS

We thank the following interviewees for their time and insight:

Martin Albert-Hoff,
Director, Operational Cybersecurity, National Security Authority

Bjarte Malmedal,
Director of Digital Security, Norwegian Business and Industry Security Council

Thor Milde,
Chief Information Security Officer, Sykehuspartner HF

Kristian S. Teigen,
Principal Engineer, Norwegian Ocean Industry Authority, Havtil

Maria Bartnes,
Program Director for Cybersecurity, DNV Group Research and Development

Arve Johan Kalleklev,
Operations Director, DNV Cyber

Anne Wahlstrøm,
Head of OT Cybersecurity Advisory Norway, DNV Cyber

UNDERSTANDING THE SOURCE OF CHART DATA

Throughout this report, we visualize data from three sources, using the following icons to signal this:

- *Critical infrastructure respondents*
- *Public respondents*
- *Threat intelligence from DNV Cyber*

SURVEY DEMOGRAPHICS

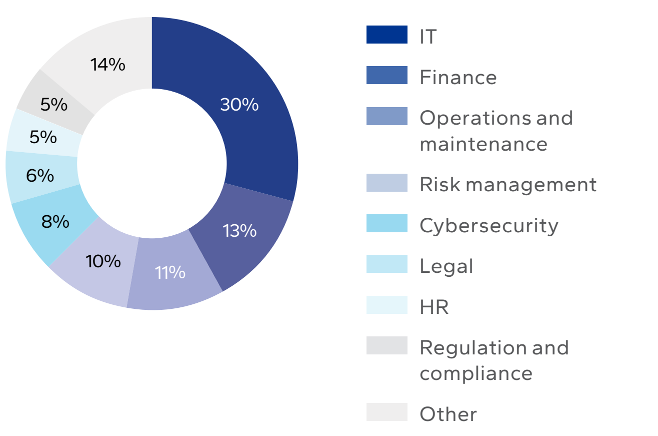
CRITICAL INFRASTRUCTURE SURVEY – NORWAY

Critical infrastructure respondents hold a range of positions, from cybersecurity-focused roles to IT experts and C-suite executives.

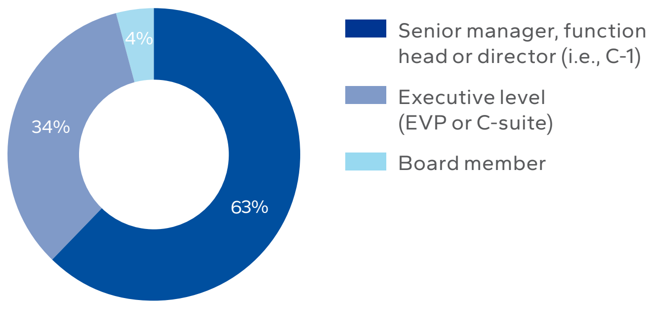
200

critical infrastructure respondents in Norway

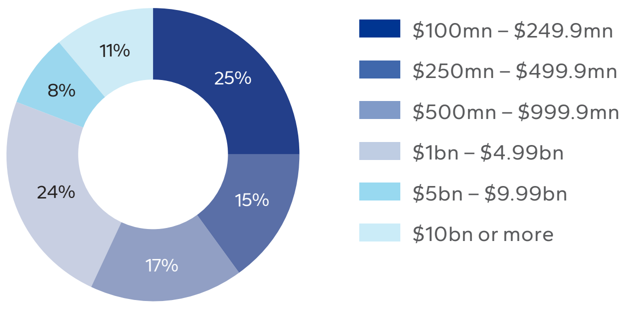
Area of responsibility



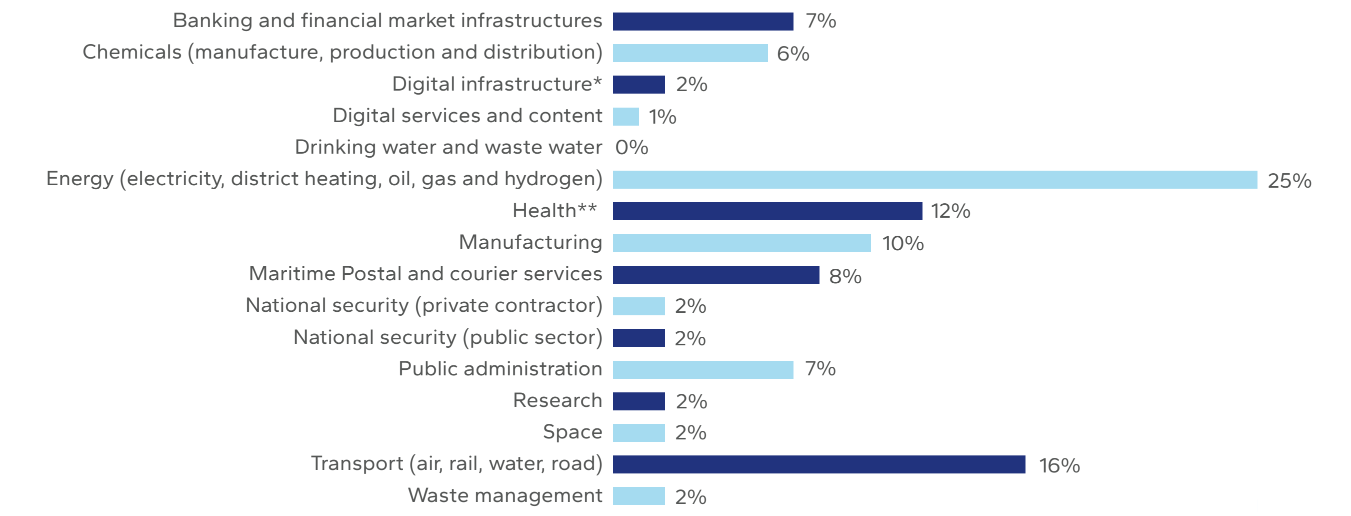
Seniority



Organization's approximate annual revenue



Sector



* Digital infrastructure includes electronic communications, trust services, domain name services, top-level domain registries, cloud services, data centres, internet exchange points, content delivery networks.

** Health includes healthcare providers, EU reference labs, research and manufacturing of pharmaceuticals and medical devices.

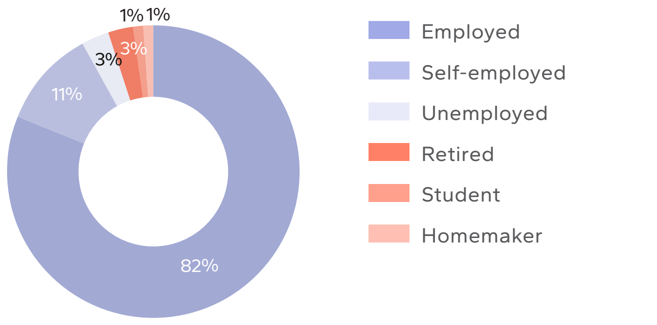
PUBLIC SURVEY – NORWAY

Public survey demographics are representative of the national population.

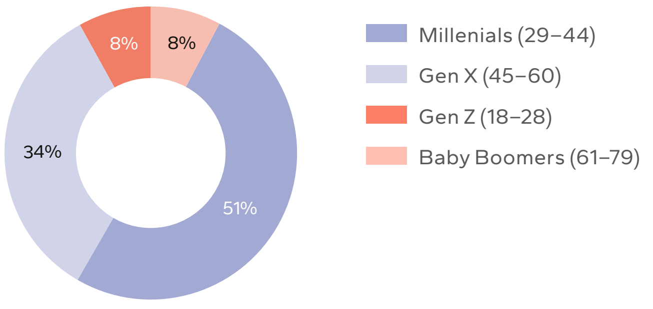
500

public respondents in Norway

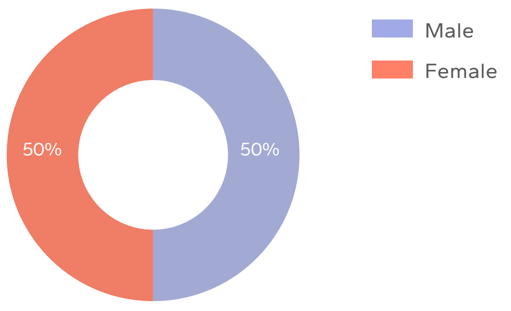
Employment status



Age



Gender



PART OF WIDER NORDIC CYBER RESILIENCE SURVEYS

As part of our wider research across the Nordics, we surveyed 800 critical infrastructure professionals and 2,000 members of the public, with respondents split equally across Denmark, Finland, Norway and Sweden.

CONTENTS

About this research 3

01 Attacks on Norway's critical infrastructure are increasing 8
Recent incidents signal a step change in outcome severity 10
Drivers of heightened cyber risk 10
Targeting the weakest link 11
Who is attacking Norway? 12

02 How prepared is Norway for a major cyber event? 16
A gap between citizens and operators 17
The national approach 18
Evolving regulation 19

03 Recommendations: Strengthening cyber resilience in Norway 20
1. Do not mistake past success for future invulnerability 21
2. Clarify responsibilities within national cyber resilience 23
3. Map supply chain vulnerabilities and sharpen visibility of third parties 24
4. Address the rising threat of more sophisticated cyber attackers 27
5. Engage the public in the country's resilience 28
6. Collaborate actively and widely to increase overall cyber resilience 32
7. Review how regulation can have the biggest impact on resilience 33

Conclusion: What secured us yesterday won't secure us tomorrow 34

References 35

01

ATTACKS ON NORWAY'S CRITICAL INFRASTRUCTURE ARE INCREASING

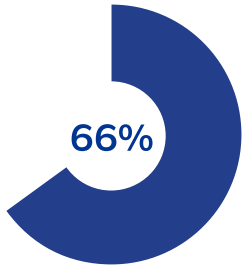
Sophisticated attacks on Norway's critical infrastructure, which is more connected than ever before, show why coordinated defence and rapid recovery abilities are increasingly crucial.

Critical infrastructure underpins every aspect of Norwegian society. Encompassing industries from energy and water to transportation, healthcare and national defence, it is integral to the nation's security, economy and public health. When critical infrastructure fails, there is almost always an impact on people, business, the economy, and society.

In DNV Cyber's new research, Norwegian executives working in these sectors report that cyber-attacks on their organizations are on the rise. Two-thirds (66%) say they have seen an increase in attacks over the past few years. Most (59%) believe that organizations in their industry are dealing with constant low-level attacks on their systems by foreign states.

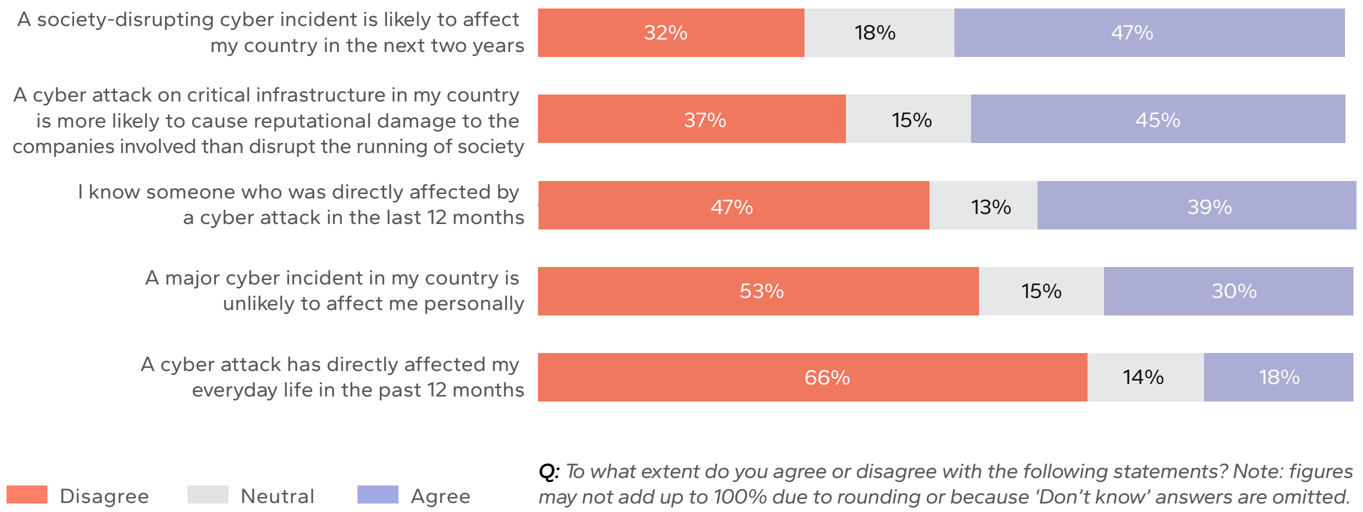
These incidents are having an impact on Norwegians' lives. Almost a fifth (18%) of the country's citizens say a cyber-attack has directly affected them in the past 12 months, and 39% personally know someone who has been affected.

> *We get a lot of things right in Norway, but we do now need to heighten our digital resilience. We need to increase security and improve our capacity to repair systems after an attack.*
>
> *Martin Albert-Hoff, Head of Operational Cybersecurity at the Norwegian National Security Authority.*



executives say they have seen an increase in cyber-attacks over the past few years.

Cyber incidents are affecting everyday life in Norway



Q: To what extent do you agree or disagree with the following statements? Note: figures may not add up to 100% due to rounding or because 'Don't know' answers are omitted.

RECENT INCIDENTS SIGNAL A STEP CHANGE IN OUTCOME SEVERITY

Norwegian awareness of cyber-attacks on critical infrastructure has grown steadily since the well-publicized 2019 Norsk Hydro incident, in which the LockerGoga strain of ransomware was used to cripple the metals company's global operations.[i] Subsequent events have bolstered this awareness. In 2024, the digital infrastructure of airport commerce operator Travel Retail Norway came to a standstill after a ransomware attack claimed by a group calling itself Akira.[ii]

These incidents were serious, but many participants in our research believe far more severe consequences are possible – and even likely. Nearly two-thirds (64%) of the Norwegian public believe that breaches of critical infrastructure could endanger life. Most executives (67%), meanwhile, think that a large-scale cyber-attack could lead to multiple, simultaneous failures of essential utilities and services.

This heightened concern could be the result of a new level of sophistication that is consistent with global powers engaging in hybrid warfare. Bjarte Malmedal, Director of Digital Security at the Norwegian Business and Industry Security Council, explains that the war in Ukraine has changed how businesses think about resilience. "The perception is certainly that risk has increased," he says. "The data may also understate the problem. When we talk to our members, it is clear that not every incident is reported."

Anne Wahlstrøm, Head of OT Cybersecurity Advisory Norway, DNV Cyber, explains how cyber-attacks can have physical consequences and potentially threaten critical infrastructure. "People used to think about cyber risk primarily in terms of compromised data but this perception has changed: attackers can gain control of physical assets," she says.

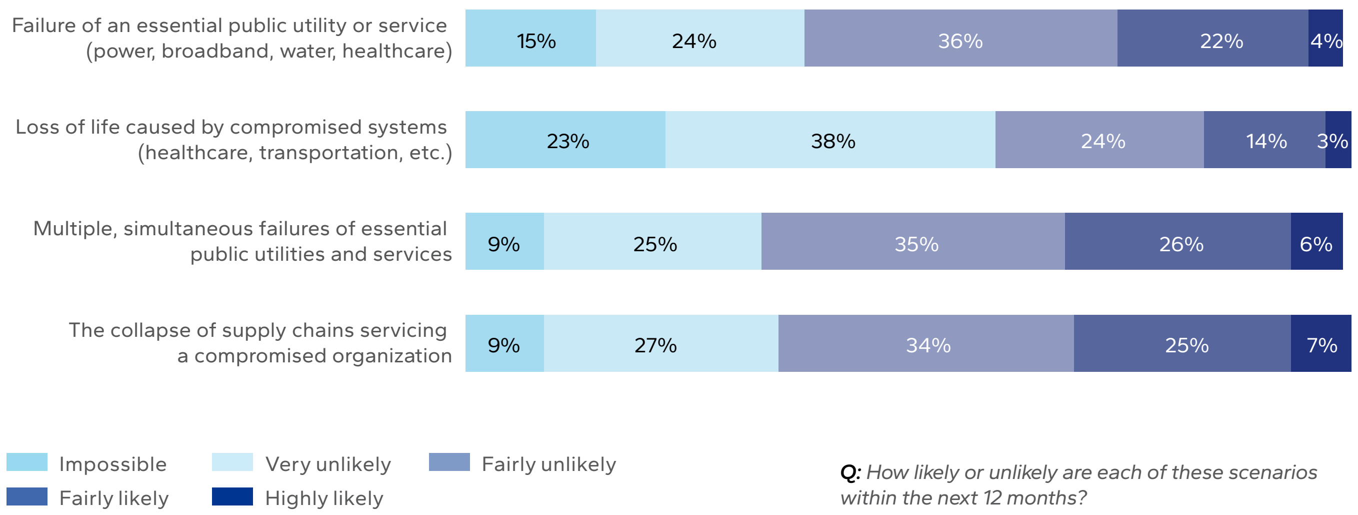
"If a hacker gains access to the digital interface controlling physical assets, they could issue commands to the system remotely. They would be able to manipulate the technology to take assets offline, or worse to cause physical changes to the asset that could endanger life, property or the environment," Wahlstrøm adds.

In the maritime sector, Oslo's Nordic Maritime Cyber Resilience Centre (Norma Cyber) has tracked hundreds of disruptive cyber incidents targeting shipping and port-infrastructure systems and warned that remote hijackings, causing physical damage, are highly feasible.[iii]

DRIVERS OF HEIGHTENED CYBER RISK

Widespread digitalization and the increased connectivity of industrial control systems (ICS), including supervisory control and data acquisition (SCADA) systems and other operational technologies (OT), have introduced new vulnerabilities into previously isolated and protected environments. This puts more pressure on Norway's most critical services, from the control of electricity supply to the treatment of water, and is therefore creating additional cyber risk.

A third of critical infrastructure professionals expect widespread disruption to supply chains and public services in 2026



Q: How likely or unlikely are each of these scenarios within the next 12 months?

"The digitalization and interconnectivity of OT is a relatively new development. Assets such as wind farms are connected to IT systems and the internet, with third parties accessing their systems to monitor and optimize operations. Sensors, navigation, and propulsion systems onboard shipping vessels are connected to IT, and then connected to the internet," says Maria Bartnes, Program Director for Cybersecurity within DNV's Group Research and Development unit. "It's not so many years ago that these technologies were air-gapped – isolated islands accessible only from a physical location such as onboard the ship. The maturity of OT security lags IT security by many years."

The organizational interdependence created by digital systems means that just one weak link can create an entry point for large-scale ransomware and data breaches, after which a hacker could move laterally to access the most valuable systems or data, and to potentially access the systems of other organizations where they are connected.

> *Supply chains are an attractive target for cyber-attacks as they provide a potential single-entry point to multiple organizations and systems, including critical infrastructure organizations.*
>
> *Maria Bartnes, Program Director for Cybersecurity within DNV's Group Research and Development unit*

"More oversight is needed, as you can't secure what you don't know. Critical infrastructure faces a heightened risk of cyber-attacks through connected networks, components, software, and third-party service providers," says Bartnes.

The impact of an attack can spiral rapidly, which may explain why executives are more likely to think an incident will result in multiple, simultaneous failures than just one failure. They think it is more likely that data corruption will spread between organizations than be contained within one system.

"Every modern company is dependent on other providers," warns Albert-Hoff. "That's why it's very important for companies, particularly in the public sector or critical infrastructure, to think not just about the cost and functionality of new services but also their security levels."

Norwegian organizations recognize that digitalization increases cyber risk, but few would argue that this outweighs the benefits. Stopping or slowing digitalization was seen by critical infrastructure executives as the least workable intervention by a significant margin: just a third (36%) say that the government should consider this option to reduce the cyber threat.

64% *of the Norwegian public believe that breaches of critical infrastructure could endanger life.*

TARGETING THE WEAKEST LINK

Along with widespread digitalization, another key driver of cyber risk is that criminal organizations may see the IT and OT environments of critical infrastructure businesses as relatively easy targets.

"In recent years, we have seen targeted attacks on the manufacturing and energy sectors," says Arve Johan Kalleklev, Operations Director, DNV Cyber. "One reason hackers target them is simply because other sectors such as financial services have invested more in strengthening their security postures. Asset-heavy businesses have often invested less, particularly in OT cybersecurity."

Kalleklev adds that attacks are growing in the healthcare sector, which hackers tended to avoid in the past. In our survey, 70% of healthcare respondents across all Nordic countries say their organizations have seen a general increase in attacks over the last few years.

Now is the time for all critical infrastructure organizations to redouble efforts to improve resilience. Concerningly our findings suggest that there are gaps in national cyber resilience, about half of critical infrastructure executives say leaders in their organizations see the resilience of critical infrastructure as someone else's responsibility.

"The weakest link in our collective resilience may not be single organizations, but the vulnerabilities created by the gaps in responsibility in securing Norway's critical infrastructure," says DNV Cyber's Kalleklev.

In that context, the next section of this report looks at levels of preparedness in the country and how government, business, and the public are sharing the burden. We then provide recommendations to help Norwegian businesses and public sector organizations overcome shared challenges and work together towards more comprehensive resilience.

Who is attacking Norway?

The threat actors that concern Norwegian critical infrastructure executives the most are organized criminal gangs. This is understandable, given the shockwaves caused by the devastating attack on Norsk Hydro in 2019 and more recent ransomware attacks by gangs on Norwegian companies.

> *The threat of ransomware attacks is what keeps me awake at night.*
>
> *Thor Milde, Chief Information Security Officer of Sykehuspartner HF.*

Sykehuspartner HF provides IT services to Norway's healthcare operators in the south-east of the country, which includes Oslo and surrounding areas where half of the Norwegian population live. "That's the sort of attack that would have the most immediate impact on our ability to deliver critical systems to hospitals," says Thor Milde, Chief Information Security Officer of Sykehuspartner HF, referring to ransomware attacks.

Norwegian companies are attractive targets for criminals because of the country's strong economic and digital foundations. As one of Europe's main energy exporters and an important participant in industries ranging from maritime to manufacturing and defence, Norway is home to many successful businesses. And with most organized cyber crime being driven by financial gain,[iv] these kinds of attacks are most likely.

"You are more likely to be attacked by a threat actor looking to make money than by a foreign state," says Mackenzie Storm, Head of Threat Intelligence at DNV Cyber . "Norwegians appear to have a clear understanding of where the real risk is coming from."

Pressure from beyond borders
Norwegian executives in DNV Cyber's research are also aware of the risk of disruption and attack connected to foreign powers. Norwegian authorities recognize Russia as the greatest threat to Norwegian security in their threat and risk assessments.[v]

"We don't yet see much of the sophisticated, state-backed attacks, but we know that the capabilities are high, which ultimately means the threat level is high too," says Kristian S. Teigen, Principal Engineer at Norwegian offshore governmental supervisory authority and regulator Havtil.

The Norwegian Police Security Service has warned that one aim of these attacks, when they do happen, is "to influence and to cause fear and chaos among the general population. Nearly half (47%) of Norwegian citizens believe that, along with organized crime, foreign powers are the most likely perpetrators of large-scale cyber-attacks on critical infrastructure.

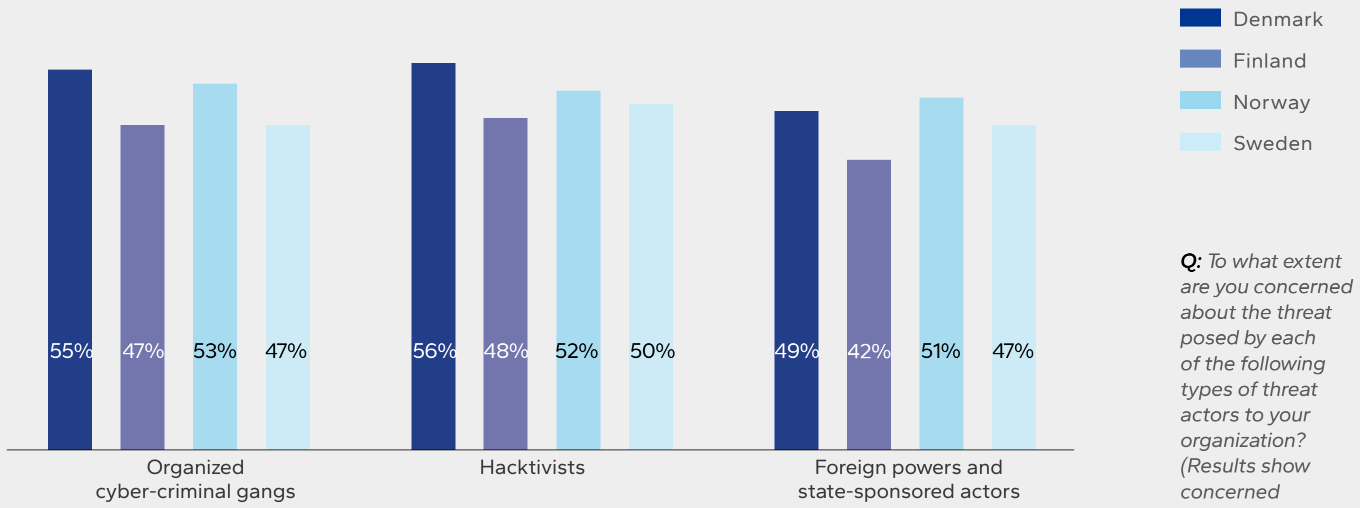
Nation states might not always carry out direct attacks themselves. They can also inspire, sponsor, or give safe haven to hackers who support political or social movements (hacktivists) and create disruption independently. Norwegian executives are as worried about the threat posed by these groups as they are about foreign powers themselves, and research suggests that pro-Russian hacktivist actors such as NoName057 and ServerKillers are active in the country.[vi]

Members of the public are less concerned about hacktivists than they are about malicious insiders, terrorist groups, foreign powers and criminal gangs (see chart). This could reflect an assumption that hacktivists act purely through ethically sound motives and pose less of a threat to human wellbeing. But this is not always the case. A 2023 cyber-attack on the Norwegian Refugee Council, for instance, in which the personal details of thousands of donors were exposed to breach, may have reflected political goals.[vii]

The lines are blurring between these threat actors. "We increasingly see hybrid attacks," says the Norwegian Business and Industry Security Council's Malmedal. "It may be a conventional type of attack such as ransomware, but supported in some way by a foreign state."

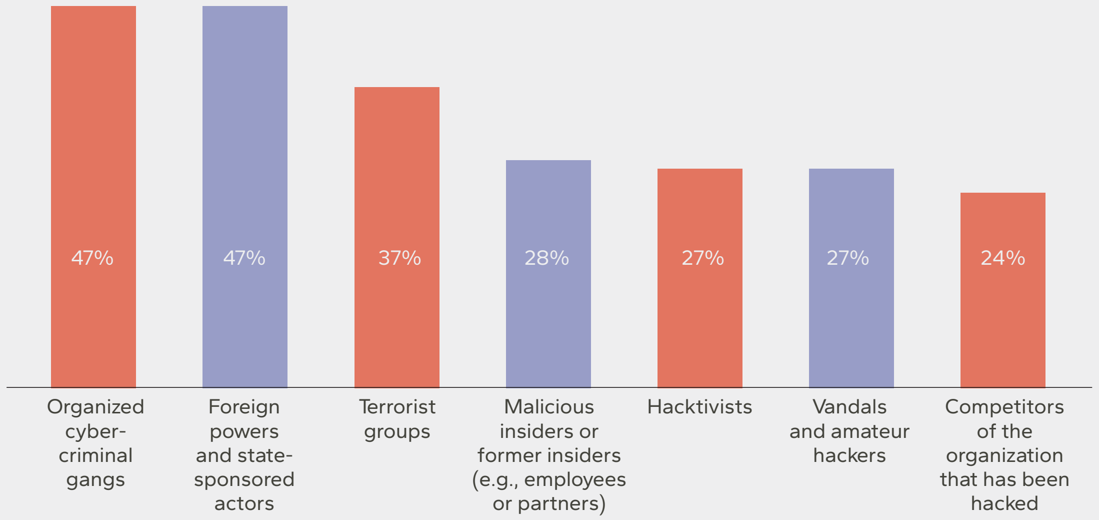
DNV Cyber Threat Intelligence tracks alleged, suspected, and confirmed attacks and breaches. Throughout 2025, we observed the following number of cyber incidents in the Nordics:
21 in Norway, 60 in Sweden,
44 in Finland, 41 in Denmark.

Critical infrastructure professionals are most concerned about organized cyber-criminal gangs, closely followed by hacktivists



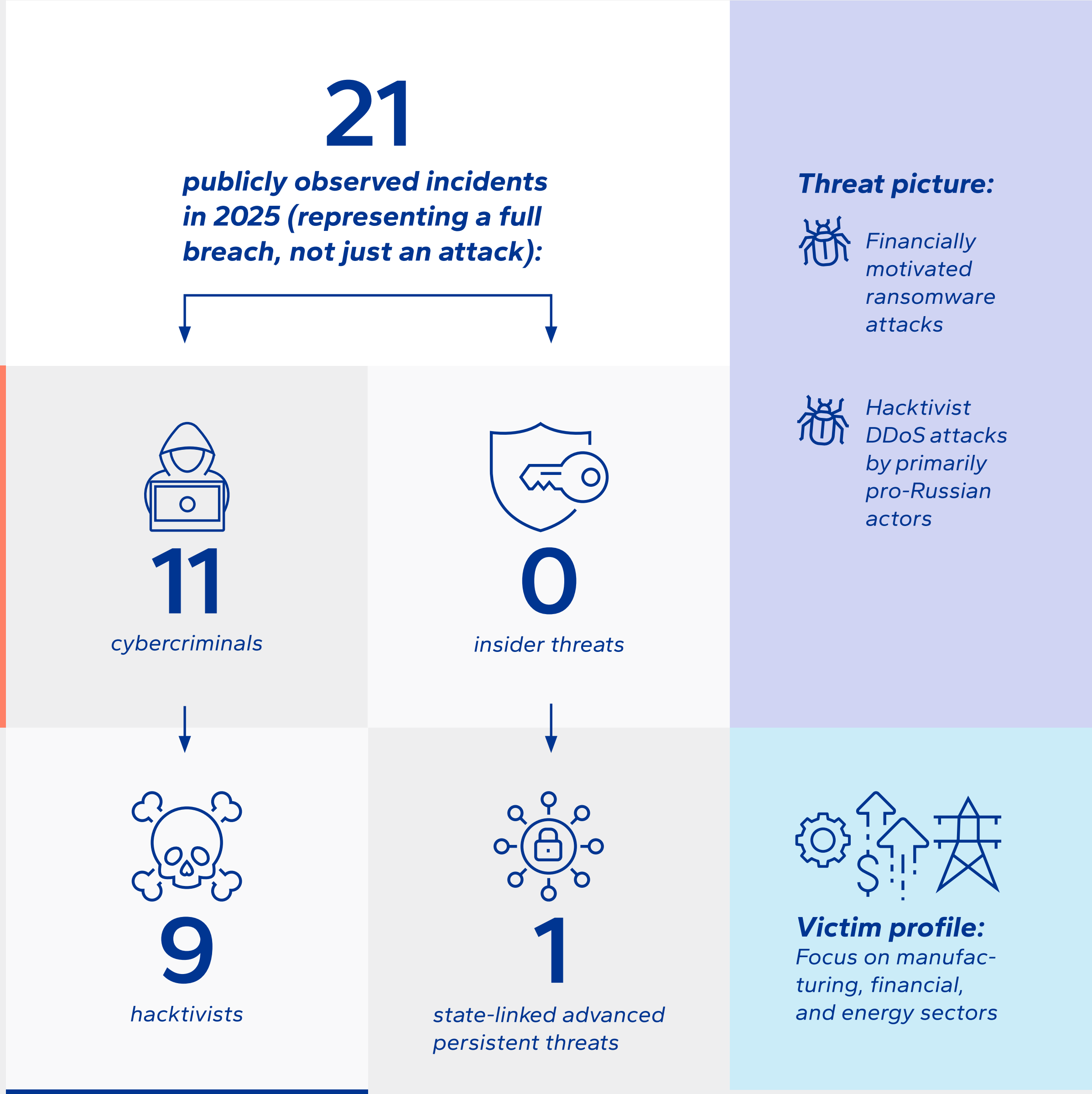
Q: *To what extent are you concerned about the threat posed by each of the following types of threat actors to your organization? (Results show concerned responses)*

The public is much less concerned than businesses are about the threat from hacktivists



Q: *Who, if anyone, do you think is most likely to carry out a large-scale cyber attack on critical infrastructure in your country at the current time?*

DNV THREAT INTELLIGENCE: NORWAY SNAPSHOT



21

publicly observed incidents in 2025 (representing a full breach, not just an attack):

11

cybercriminals

9

hacktivists

0

insider threats

1

state-linked advanced persistent threats

Threat picture:

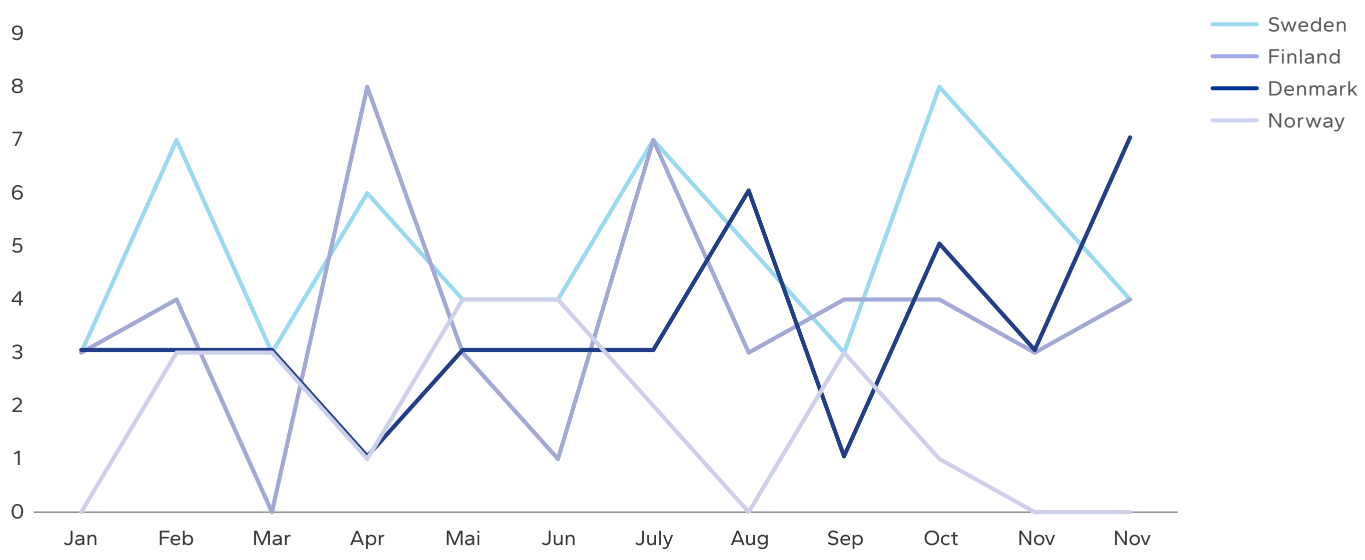
Financially motivated ransomware attacks

Hacktivist DDoS attacks by primarily pro-Russian actors

Victim profile:

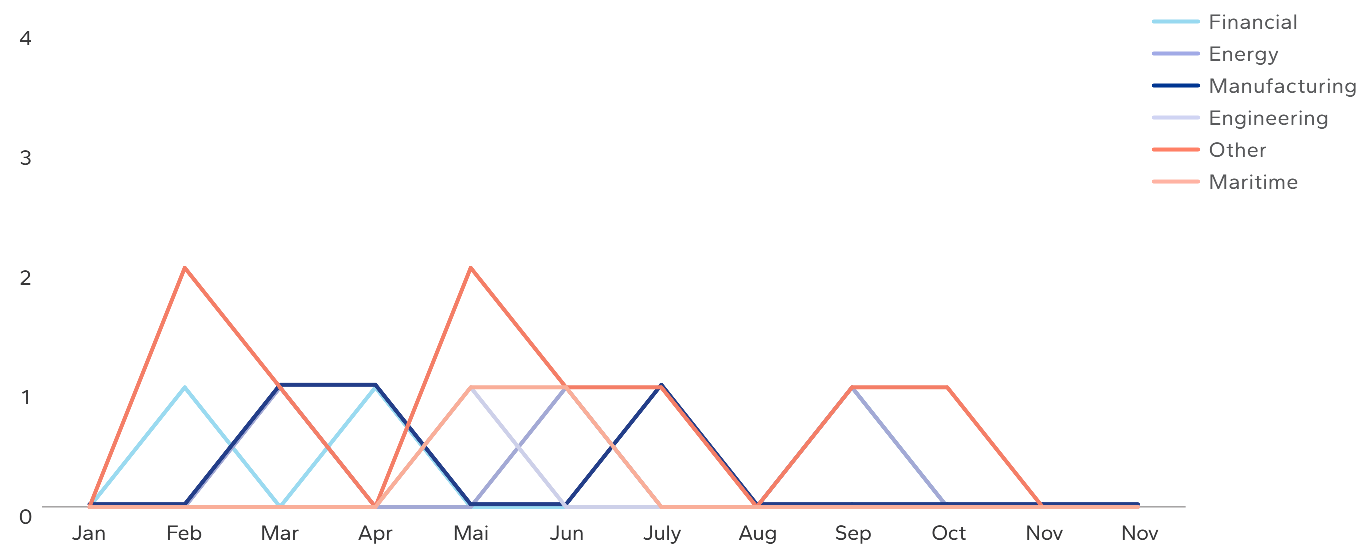
Focus on manufacturing, financial, and energy sectors

Cyber incidents in Norway over 2025, compared to other Nordic countries

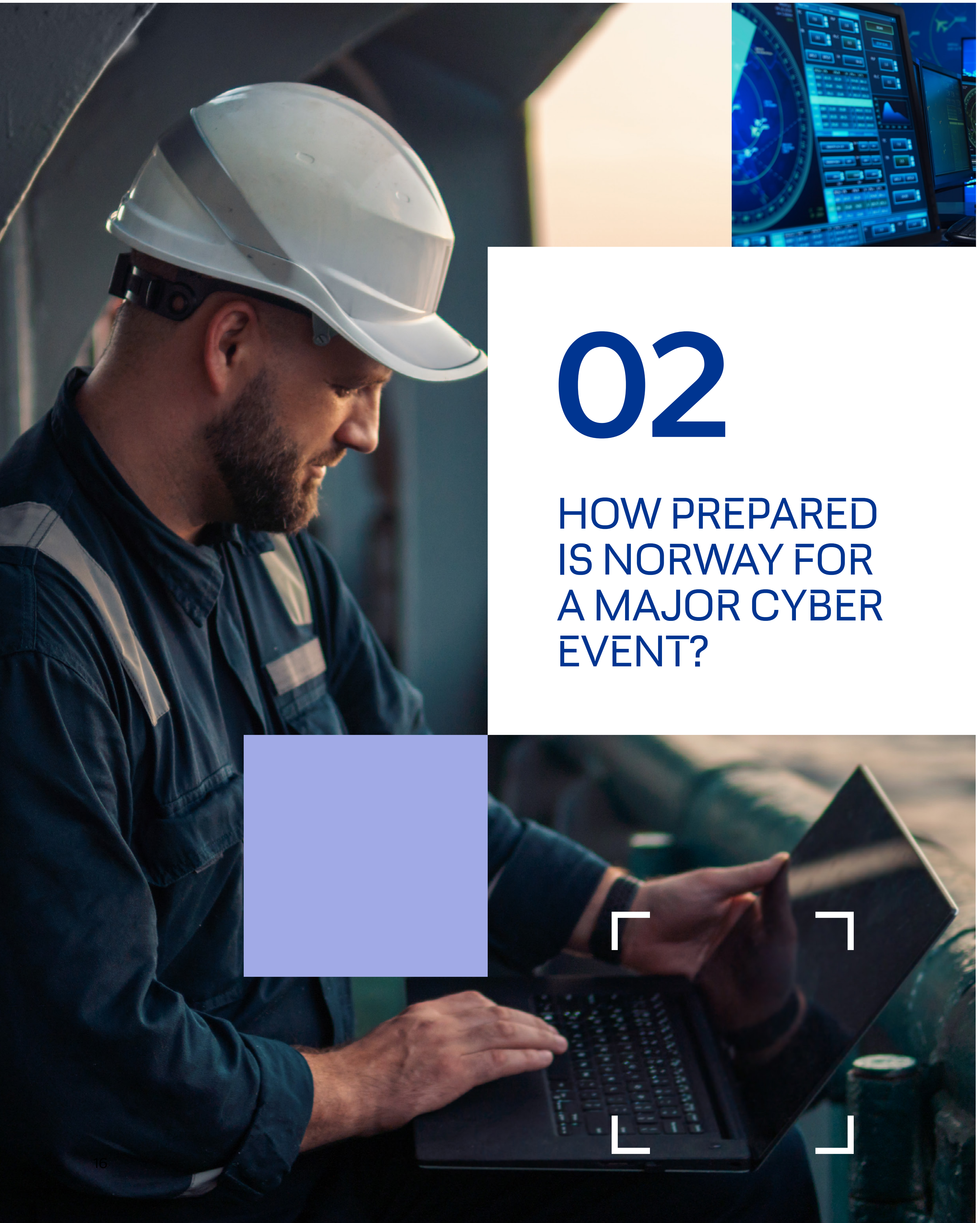


DNV Cyber Threat Intelligence: Data points represents the number of "cyber incidents" observed during the month per country, such as ransomware attacks, access sales, or data breaches. A single hacktivist data point often represents multiple incidents as these actors tend to target multiple organizations with DDoS attacks at once

Cyber incidents in Norway over 2025, by industry



DNV Cyber Threat Intelligence: Data points represents the number of "cyber incidents" observed during the month per selected sector, such as ransomware attacks, access sales, or data breaches. A single hacktivist data point often represents a larger DDoS campaign.



02

HOW PREPARED IS NORWAY FOR A MAJOR CYBER EVENT?

Norway is strengthening its national cyber response and regulation, which is helping to reassure the public. But among critical infrastructure organizations, preparedness and accountability is uneven.

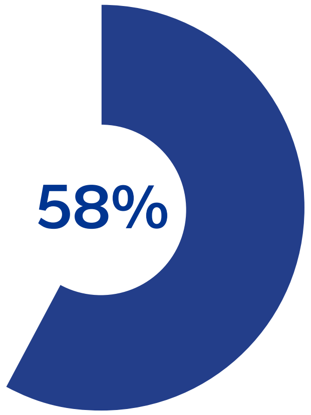
Just over half of Norwegian citizens (53%) expect they would be personally affected by a major cyber incident in their country. Among critical infrastructure executives, about six in 10 (58%) believe a cyber-attack could feasibly lead to political, economic or military retaliation against another country in 2026.

So, how prepared is Norway? The picture that emerges from our research is one of a country that has taken impressive steps towards building a coordinated national response and regulatory framework. But barriers linger further down the chain. Many organizations are not confident in their own defences, which undermines the resilience of the system as a whole.

A GAP BETWEEN CITIZENS AND OPERATORS

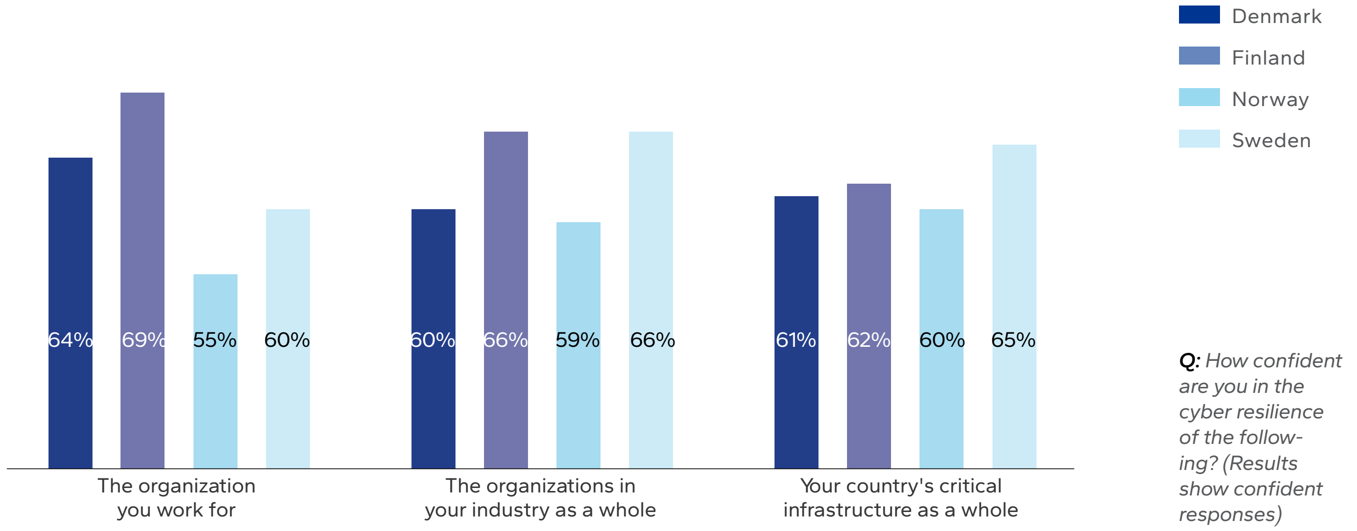
Our research suggests that Norwegians overall are confident that the powers that be are working effectively to manage the cyber risk to critical infrastructure. Norwegian citizens are the most likely across the Nordics to believe that their country's critical infrastructure systems are safe from cyber-attack (57%) compared with a Nordics average of 48%). They are also significantly more likely to believe that their country is better than other European nations at keeping its critical infrastructure secure (54% compared with 46%).

Is this assessment of Norway's resilience accurate or could it be that the public are unaware of the reality of the situation? To answer that question, it is worth noting that the Norwegian public are the most confident (72%) across the Nordics in their knowledge of the people and organizations responsible for protecting their country's critical infrastructure They are also broadly aligned with the executives in our research, more than two-thirds of whom feel reasonably favourable towards the cyber resilience of the government.



executives believe a cyber-attack could feasibly lead to political, economic or military retaliation against another country in 2026

Norwegian critical infrastructure professionals are less confident about their industry's cyber resilience than peers in other Nordic countries



Q: *How confident are you in the cyber resilience of the following? (Results show confident responses)*

Confidence among Norwegian executives is not consistently positive. They are the least likely to express high confidence in the resilience of their own organizations (55% compared with a Nordics average of 62%). This helps explain why they are generally less sure about the resilience of their industry and the country's critical infrastructure as a whole. If almost half of organizations are uncertain about their own resilience, it follows that confidence in the wider system will also be uneven.

Moreover, some may not even feel that they have a part to play in this resilience. About one in two (52%) critical infrastructure executives admit to having colleagues who think national critical infrastructure resilience is a challenge for other people, and they themselves will not be held accountable.

55%

Norwegian executives are the least likely to express high confidence in the resilience of their own organizations (compared with a Nordic average of 62%)

THE NATIONAL APPROACH

Who are these "other people"? When it comes to direct incident response, the Norwegian National Security Authority (NSM) is the country's dedicated agency for cyber resilience. Both nationally and internationally, it is the official point of contact for ICT threats and cybersecurity incidents. The security authority also serves as the base for Norway's computer security incident response team, NorCERT.

> *We hold the national response function for cyber operations across both the public and private sectors, including civilian and military defence. The fact that we have this overarching role is a huge advantage for Norway, because it means we can have a holistic approach to maintaining the situational awareness around cyber, as well as in how we handle responses. It allows us to see the broader threat picture.*
>
> *Martin Albert-Hoff, Director, Operational Cybersecurity, National Security Authority*

In addition to the National Security Authority, which is responsible for handling serious cyber incidents across the country's critical infrastructure, Norway is home to several independent, sector-specific CERTs.

executives admit to having colleagues who think national critical infrastructure resilience is a challenge for other people, and they themselves will not be held accountable.

These include the health and care-focused HelseCERT, KommuneCERT for the municipal sector and KraftCERT for power and petroleum. There is also the Nordic Financial CERT, a private, nonprofit organization working to improve industry collaboration across the Nordics.[viii]

EVOLVING REGULATION

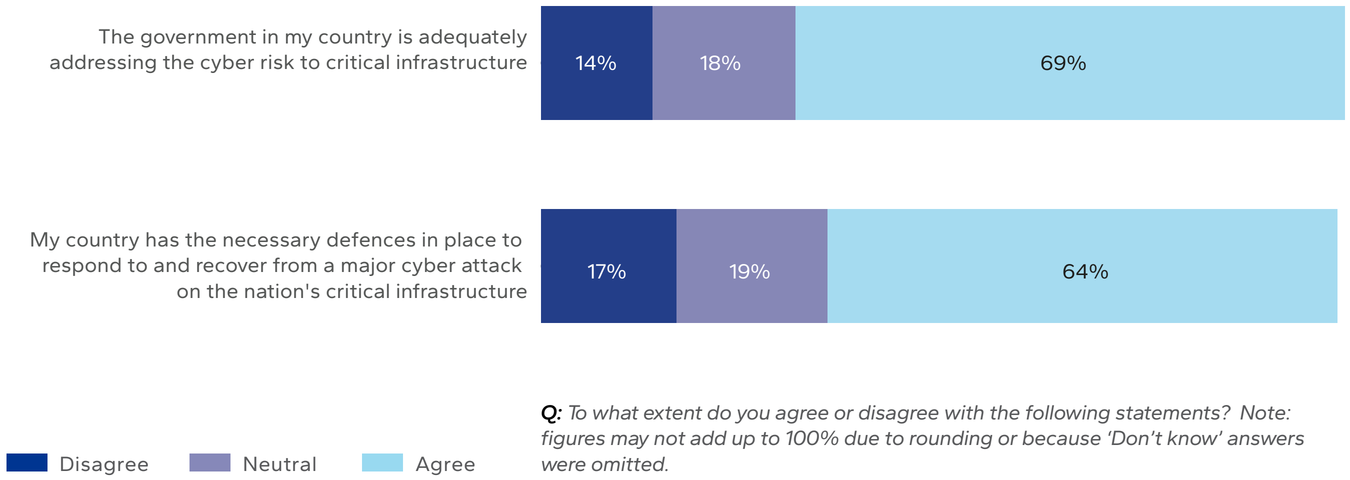
In 2019, the government launched the National Cyber Security Strategy for Norway. This built on Norway's long-standing Security Act (Sikkerhetsloven), which was first introduced in 1998 and updated in 2018.[ix] Over time, the country also implemented various sector-specific regulatory frameworks. Its security regulation for the power sector, for example, was first established in 2002, before the power preparedness regulation (Kraftberedskapsforskriften) came into force in 2012.[x] In the 2019 National Cyber Security Strategy, the Norwegian government outlined its plans to tackle new and existing security challenges in critical infrastructure by developing new regulation, supervisory activities, guidance and enhanced collaboration.[xi]

It has made important progress. In October 2025, it implemented the Digital Security Act, which mandates risk-based security measures, incident reporting, and increased oversight for providers of essential services such as energy, transport, and health and digital services. The regulation aligns Norway with European Union standards such as the NIS1 Directive, and holds senior leaders accountable for digital resilience and the protection of critical infrastructure and digital services.[xii]

The development of well-designed and effective regulation is the area where critical infrastructure executives say they have seen the most progress. Compliance should, however, be seen as the baseline on which to build rather than the desired result. "Individual organizations must assess the specific threat level they are facing and develop their own response accordingly," says Maria Bartnes, Program Director Cybersecurity, DNV.

For Norway to achieve full resilience, government, operators and the wider ecosystem must work together towards a common goal. Responsibility for protecting Norway's critical infrastructure must be shared.

Executives are largely confident in the government's ability to protect the country's critical infrastructure from cyber risks



Q: *To what extent do you agree or disagree with the following statements? Note: figures may not add up to 100% due to rounding or because 'Don't know' answers were omitted.*

03

RECOMMENDATIONS: STRENGTHENING CYBER RESILIENCE IN NORWAY

Norwegian society understands the need to enhance the cyber resilience of critical infrastructure as part of creating a more resilient nation state.

> *We need to recognize that there is a difference between some of the attacks of the past and a major attack on our critical infrastructure mounted by those with really serious capabilities. We must be prepared for that.*
>
> *Kristian S. Teigen, Principal Engineer, Norwegian Ocean Industry Authority, Havtil.*

In this section, we provide recommendations on what needs to happen for Norway to continue its trajectory towards a more mature level of cyber resilience.

Indeed, nuances in the survey data and expert commentary reveal challenges that everyone must first come together to address, with implications for business, government and society.

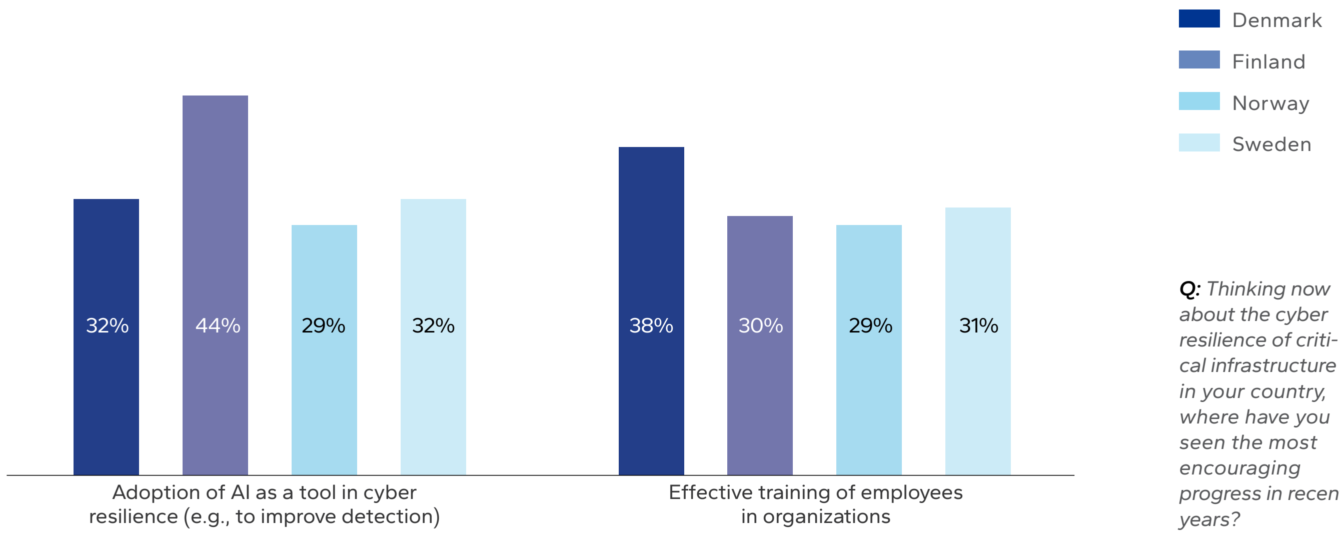
1. DO NOT MISTAKE PAST SUCCESS FOR FUTURE INVULNERABILITY

Cyber risk management successes are worthy of celebration, but they do not guarantee new threats will be detected and repelled. That requires a fresh commitment to resilience.

More than half (55%) of Norwegian critical infrastructure executives are optimistic about the defences their organizations have established, even if this proportion is lower than in the other Nordics countries. Concerningly, however, their optimism could be based on an outdated view of resilience. Asked why they are confident, executives are most likely to say that their organizations have a strong track record of responding quickly to attacks or of recovering rapidly from incidents.

This 'hot streak' mentality may contribute to a false sense of security. Organizations that fended off attackers in the past cannot assume they will be able to do so again, especially as attacks become more regular and more sophisticated. Norway may have been an early adopter of digital defence techniques, but by relying on past capabilities it risks being overtaken by the countries that are catching up now. For example, executives in Norway are less likely than their counterparts in other countries to say they have made positive progress on training employees on cybersecurity. Many cyber-attacks are still caused by human error, so this is a real danger.

Only a third of Norwegian critical infrastructure professionals is happy with the rate at which AI is being adopted as a cyber resilience tool



Q: Thinking now about the cyber resilience of critical infrastructure in your country, where have you seen the most encouraging progress in recent years?

> *We still see that most attacks happen where the initial vector of entry is something as easy as a bad password or unpatched system that should have been fixed a long time ago. The adversary will choose the easiest and cheapest path to its goal, so it's vital that companies complete the basics of cybersecurity before moving on to expensive mitigation tools.*
>
> *Martin Albert-Hoff, Director, Operational Cybersecurity, National Security Authority*

It is striking that Norwegian organizations have made less progress than those in other Nordic nations in adopting AI as a tool for cyber resilience, even though its advantages include real-time threat detection and automated log analysis. Only 29% of executives say they have seen positive progress in this area, compared with an average of 34% across surveyed countries. As with training employees, it appears some businesses have fallen into the trap of assuming that because they have successfully defended themselves in the past, they no longer need to evolve their approach to resilience.

Reset expectations

Norwegian businesses must renew their commitment to resilience to keep up with the accelerated threat. "Part of that is simply having a Plan B," says Thor Milde of Sykehuspartner. "What will you do if your primary system or service provider fails?"

Other areas of focus could mean increased training for employees at every level of the organization. Norwegian businesses are lagging behind, but help is available. The Norwegian National Security Authority, for example, provides advice and support on cyber training.

29%

executives say they have seen positive progress in adopting AI as a tool for cyber resilience

2. CLARIFY RESPONSIBILITIES WITHIN NATIONAL CYBER RESILIENCE

Among Norwegian executives working in sectors considered critical by the EU, over half (52%) say that leaders in their organization see resilience of critical infrastructure as someone else's responsibility. A third (32%) are not even clear on whether their organization is involved in critical infrastructure.

At the same time, trust in Government to manage cyber threats is high, as seven in ten executives (69%) believe authorities are handling the digital risk to critical infrastructure sufficiently. There is support for further Government action, as six in ten executives (60%) back stricter cybersecurity regulation, while many (63%) believe it is necessary to impose politically sensitive measures affecting the public (such as greater surveillance of public data).

Support is similarly strong among the public as two thirds of Norwegian citizens (64%) believe authorities should have more powers to stop cyber-attacks, even if this means breaching consumer privacy.

Confidence in government is positive, but it can also lead to a false sense of security and present gaps in responsibility.

> *The Government can set expectations, enforce accountability, share intelligence, encourage cooperation, and build public awareness, but they cannot directly secure infrastructure they do not own"*
>
> *Arve Johan Kalleklev, Operations Director, DNV Cyber.*

"Cyber resilience depends on how well businesses, the public, and authorities each understand and fulfil their role in an interconnected system. We must all take responsibility for Norway's critical infrastructure," says Kalleklev.

Three-quarters (72%) of Norwegian executives say greater clarity is needed on the role their organizations are expected to play in securing our critical infrastructure.

"We should rightly consider the cyber threats we face and our preparedness, but it's time we also discussed who exactly is responsible for managing these risks and what role we each should play," adds Kalleklev.

The Government recognizes the need to mobilize the private sector in its Total Preparedness report (Totalberedskapsmeldingen[xiii]).

3. MAP SUPPLY CHAIN VULNERABILITIES AND SHARPEN VISIBILITY OF THIRD PARTIES

Organizations' suppliers create multiple points of weakness that attackers could strike. Mapping these points and eradicating them is an imperative.

While the inherent benefits of digitalization are undeniable, modernization has led to an expanding attack surface for every organization. Gaps and weaknesses in the supply chain, such as a supplier, contractor or other third party, can provide easy access points and the means for a malicious actor to infect the whole network.

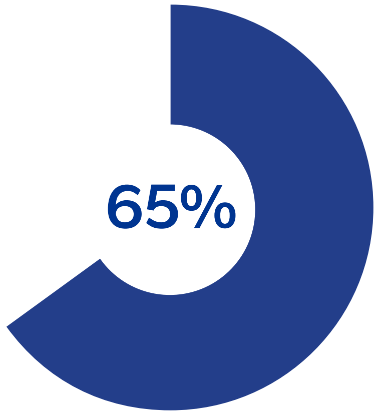
The complexity of the supply chain makes it difficult for organizations to monitor the dependencies and connections that increase vulnerability. For example, a retailer has limited visibility into the specific security measures of the company that provides its payment solutions.

"What we often see is that dependencies are underestimated, especially in the supply chain," says Havtil's S. Teigen.

In our research, Norwegian executives have far less confidence in the resilience of their suppliers – both their immediate suppliers and subsequent tiers – than in other parts of the industry. This partly reflects their lack of visibility and inability to verify the cyber resilience of their connections remotely.

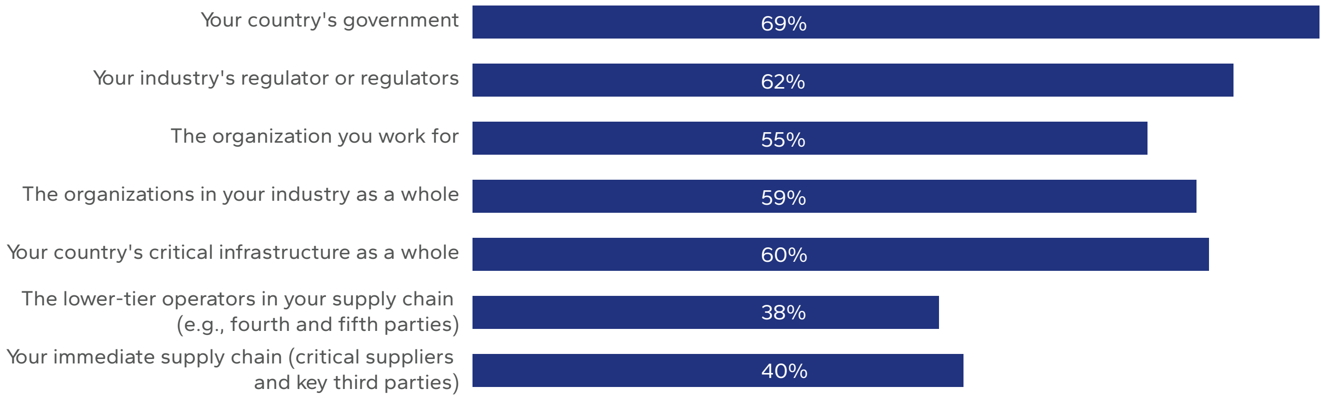
"We constantly feel that we should spend more time on this area," says Sykehuspartner's Milde. "Even though we have a long list of security requirements for vendors, some parts of healthcare are niche. You have to be pragmatic and focus on the big risks, because otherwise you may end up with no provider at all."

The exposure here is significant. Almost two-thirds (65%) of critical infrastructure executives believe it would have an immediate impact on their ability to operate if their key external providers were breached. Yet less than half (47%) are well prepared or very well prepared for a successful attack disrupting their supply chain.



of critical infrastructure executives believe it would have an immediate impact on their ability to operate if their key external providers were breached

Critical infrastructure professionals lack confidence in the cyber resilience of their suppliers



Q: How confident are you in the cyber resilience of the following? (Results show confident responses)

Increase visibility and control

"Companies need to get better at mapping how the exploitation of one weakness in the system can impact the business," says S. Teigen. "This starts with a thorough review of the supply chain to make sure that organizations have better visibility of where they are exposed."

Organizations can use this transparency to assess cyber risk and eliminate weak points. "It may be necessary to renegotiate contracts to give suppliers more responsibility," says Malmedal of the Norwegian Business and Industry Security Council. This will become increasingly important, as the Digital Security Act extends organizations' cyber responsibilities to also factor in the cybersecurity of their suppliers.[xiv]

> *Any company acquiring services from a third party should demand a certain level of security."*
>
> *Martin Albert-Hoff, Director, Operational Cybersecurity, National Security Authority*

"Don't only think about the cost and functionality of the services provided, but also about how secure they are," says the National Security Authority's Albert-Hoff.

Regulation and cybersecurity standards have a key role to play in setting a baseline for security, but companies themselves also need to drive security through their supply chains.

"Businesses should set cybersecurity requirements for suppliers based on their company's risk profile, including in procurement, supplier contracts, and the design of processes and assets," says DNV Cyber's Wahlstrøm. "They should also check on the actual implementation of those requirements, and test and enhance detect and response capabilities together with suppliers."

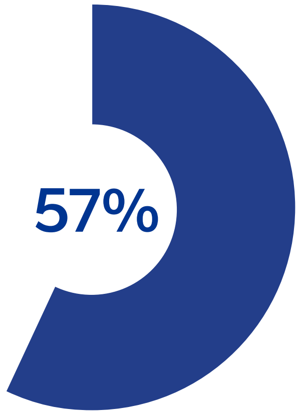
Organizations can also mitigate supplier risk with defensive tactics such as zero trust principles and vulnerability detection. These can stop problems that occur at a supplier from spreading to the organization itself.

Finally, businesses that own or use operational technology should be acutely aware of how and where they are

connected, with suppliers often requesting ongoing connectivity for maintenance and updates. "We've had to be hard on vendors," says Sykehuspartner's Thor Milde. "We want to isolate devices to protect our network which make it challenging for vendors from a service and maintenance perspective. Vendors can't simply have open access. It needs to be done in a secure manner."

While this connectivity enhances efficiency and innovation, each identity represents a potential entry point for cyber criminals.[xv]

"A single compromised identity – human, or non-human in the case of applications, bots and AI – can enable threats to access critical systems, and even to move laterally to other critical systems," says Wahlstrøm. "By securing digital identities, companies can reduce the risk by enforcing precise, risk-adaptive access controls: only the right people and machines get access to systems, at the right time, with the least privilege needed."



executives say their business depends on suppliers based in countries where geopolitical tensions are rising.

54%

are so concerned that they think it may be necessary to move manufacturing and third-party services to allied states.

Managing geopolitical risk in supply chains
More than half of executives (57%) say their business depends on suppliers based in countries where geopolitical tensions are rising. A narrow majority (54%) are so concerned that they think it may be necessary to move manufacturing and third-party services to allied states.

A case in point is Europe's energy system. This is vulnerable because its OT cyber defences are lagging, as demonstrated by the coordinated attack on Poland's energy system in the middle of a cold spell in December 2025[xvi]. Hackers targeted at least 30 wind and photovoltaic farms, a private manufacturing company, and a combined heat and-power plant, exploiting exposed network devices as well as other vulnerabilities.

Such network devices are also vulnerable via the supply chain. Energy companies must contend with the risk of procuring components containing software that could have been compromised before delivery. In the renewables sector, for example, wind and solar companies rely heavily on specialist manufacturers to provide components with embedded sensors and supervisory control and data acquisition systems (SCADA).

China continues to set renewables buildout records with a 56% global share of new solar PV capacity and 60% share of wind power globally, according to DNV's Energy Transition Outlook 2025 report[xvii]. A recent report produced by DNV for SolarPower Europe addressing cybersecurity risks to the EU energy sector, suggests it may be necessary to limit remote access and control of solar PV systems from outside the EU[xviii].

"Supply chains are the 'weak underbelly' in cyber resilience," explains DNV Cyber's Wahlstrøm. "Critical organizations need to manage the geopolitical risk in supply chains, but they also need to address the wider issue of vendor concentration and dependence. If all companies have agreements with the same limited number of suppliers and IT vendors, our critical infrastructure will be more vulnerable."

4. ADDRESS THE RISING THREAT OF MORE SOPHISTICATED CYBER ATTACKERS

Norway may not yet have grasped sophisticated adversaries' involvement in cyber-attacks. The government must work harder to protect Norwegian interests.

Geopolitical tension is increasing the threat of state-sponsored cyber-attacks, even if this currently is not the most common threat that critical infrastructure Norwegian operators encounter. Analysis by the Center for Strategic & International Studies suggests that the number of these attacks originating in Russia tripled between 2023 and 2024.[xix]

"The threat level in Norway is higher than ever because Norwegian oil and gas plays such a critical part in Europe's economy," says Havtil's S. Teigen. "Norway's broader support of Ukraine also puts it in the firing line."

However, the Norwegian public are less likely than people in neighbouring countries to believe that a society-disrupting cyber incident could affect their country in the next two years. And Norwegian executives are less likely than those in Sweden and Finland to believe that this kind of event could harm their country's economy.

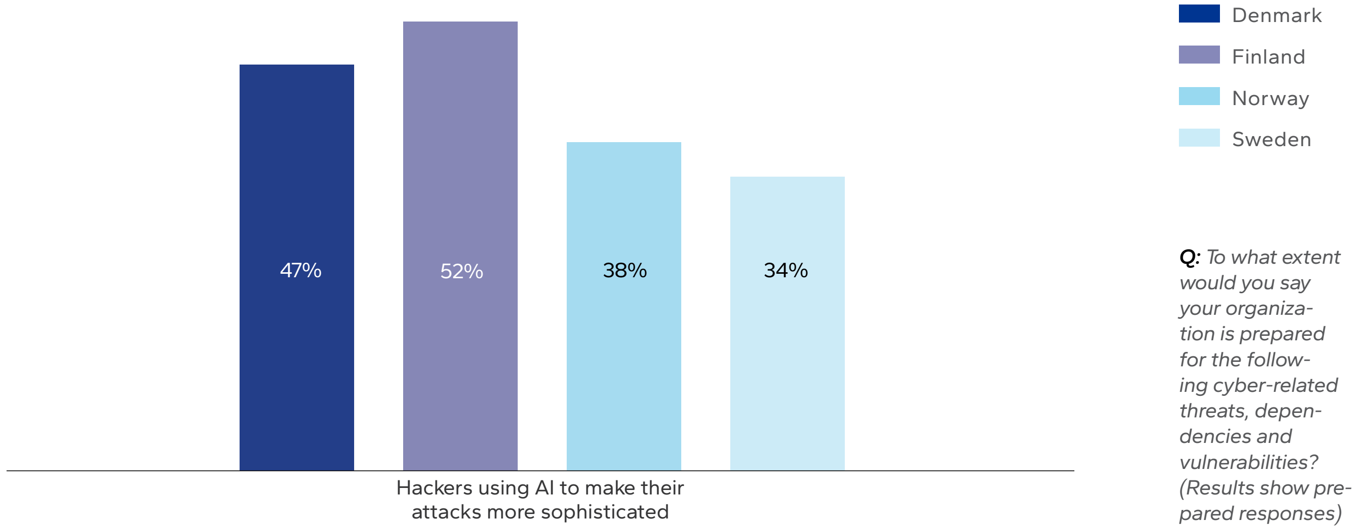
It could be that they are underestimating just how rapidly the capabilities of attackers are advancing. Cybercrime-as-a-service, a business model in which skilled cybercriminals offer tools and expertise for sale, enables those with limited technical ability to carry out attacks. And where it used to take hackers weeks to move from vulnerability discovery to exploitation, the growing use of AI means they can now do it in days.[xx] Despite this, only two in five infrastructure organizations in Norway say they are prepared for hackers using AI to make their attacks more sophisticated.

Build awareness and understanding
There are steps businesses can take to navigate these evolving dangers. They can improve their technical knowledge of the use of AI by cyber attackers, and they can use AI in their own cyber defences. A growing number of tools harness the technology.

Norway's government should also do more to support the critical infrastructure organizations that are being targeted for strategic reasons. They are the victims of attacks that ultimately target Norwegian society itself, rather than individual businesses.

That might mean increased intelligence-gathering and information-sharing by the country's security agencies and cyber crime specialists. It could mean state action against groups that are sponsored by foreign powers; for example, through international cooperation across law enforcement agencies. The government could also increase workforce training in AI and cyber skills to increase the number of people who can protect organizations.

Only two in five Norwegian critical infrastructure organizations are prepared for hackers' increasing use of AI



***Q:** To what extent would you say your organization is prepared for the following cyber-related threats, dependencies and vulnerabilities? (Results show prepared responses)*

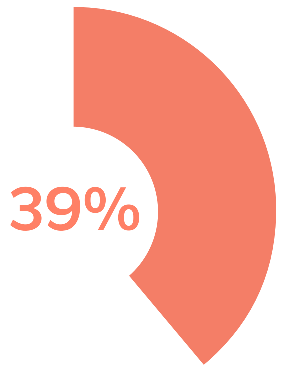
5. ENGAGE THE PUBLIC IN THE COUNTRY'S RESILIENCE

The Norwegian public feel they have a good understanding of cyber risk. Now, they might need to question those assumptions.

Many Norwegians feel that they can make a difference to their country's cyber resilience: just 39% say they cannot do much to reduce the risks of a cyber-attack on critical infrastructure. In other Nordic countries in this research, the total percentage of people disclaiming responsibility is higher: 50% in Sweden and 43% in both Denmark and Finland.

Gen Z citizens are the most sure that they have a role to play in protecting the country's critical infrastructure (18% say they cannot do much), while Baby Boomers appear to be much more passive (66%). This difference may stem from younger 'digital native' generations growing up with technology and being more aware of the risks involved, whether that's online safety or misinformation. By contrast, older generations may be more used to a society that is less connected, potentially leading to a stronger sense that responsibility lies with the state and service providers rather than individuals.

Either way, Norwegian citizens believe that they would cope well in the event of a major disabling attack (see charts). In addition, a majority say they are always able to spot attempts by hackers to target them, and that they would know what to do if their personal details were used to carry out an attack.



say they cannot do much to reduce the risks of a cyber-attack on critical infrastructure

But are they overconfident? Executives in the critical infrastructure sector are not so convinced of the public's understanding and awareness. For example, 47% say that the Norwegian public is not as aware as it should be about how severe the impacts of a major cyber incident could be.

It may be that Norwegians are now well-versed in everyday cyber threats. As we have seen, significant numbers of Norwegians have been targeted by cyber attackers or know someone who has. They may also have a strong belief that a culture that prioritises collective responsibility, such as Norway's, will encourage people to support each other during a crisis. But this is not the same as recognizing and preparing for the systemic threat of sophisticated, large-scale attacks on the country's critical infrastructure.

> *We need a holistic approach where Norwegians are secure both at home and at work – across their whole digital life.*
>
> *Bjarte Malmedal, Director of Digital Security, Norwegian Business and Industry Security Council*

This is becoming even more important as the lines between personal and professional lives continue to blur. As individuals increasingly use both their own devices in the workplace and work devices in their personal lives, vulnerabilities in personal security expose their organizations to the risk of a cyber-attack.

And Norwegians are increasingly using personal devices as their point of access to certain parts of the country's infrastructure. Most (70%) have an online banking app on their smartphone, and more than a third (37%) have an app they use to manage the charging of their electric vehicles. These points of entry provide attackers with further nodes to explore as they probe for weakness – and they are nodes that people might not realize they need to protect.

"The rise of consumer apps and smart home equipment is providing attackers with more opportunities to breach critical infrastructure," says DNV Cyber's Kalleklev. "It is all part of a chain. By infiltrating these devices, threat actors can use them in a DDoS attack and put massive and potentially crippling pressure on energy grids, banking infrastructure or other essential systems."

Empower the public

Some executives, perceiving public overconfidence, might feel frustrated . But there is an opportunity here to recruit Norwegian citizens to protect their country's critical infrastructure. The government can lead that recruitment. Two-thirds of executives (67%) believe more investment is necessary to make the public aware of their role in supporting national cyber resilience.

When they do invest, policymakers also need to carefully balance the tone and content of campaigns, without stoking unnecessary fear and distrust. Educating the public about actions they can take, from multi-factor authentication and segmentation to password managers, is likely to be more effective at stopping attacks than spreading fear about hostile foreign powers, for example. But it is important that people understand what is expected of them in the case of a larger, more disruptive attack.

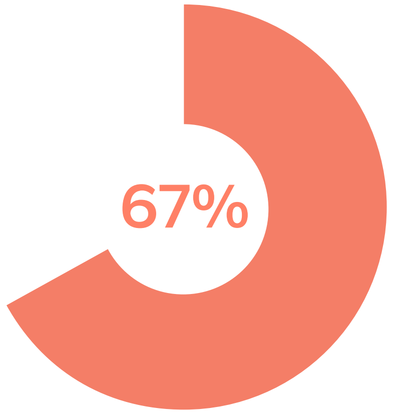
High confidence in the government and Norway's longstanding NATO membership may have left citizens feeling safer. But to avoid public complacency, policymakers will need to encourage citizens to question their assumptions without creating a climate of fear.

The "Iberian Blackout" in April 2025 led to a power failure across the Peninsula and brought to light critical challenges in crisis coordination and society preparedness.

A key part of this will also be to create understanding of the damage attacks can do to affected organizations. Currently, most members of the Norwegian public (67%) think companies should be able to fully restore their systems within a few hours after a major cyber-attack has taken place. And more than half believe that organizations can fully prevent cyber-attacks by installing the correct software in their computer systems. This implies that citizens still overwhelmingly think of cybersecurity as a technical challenge, rather than a risk that carries widespread societal implications.

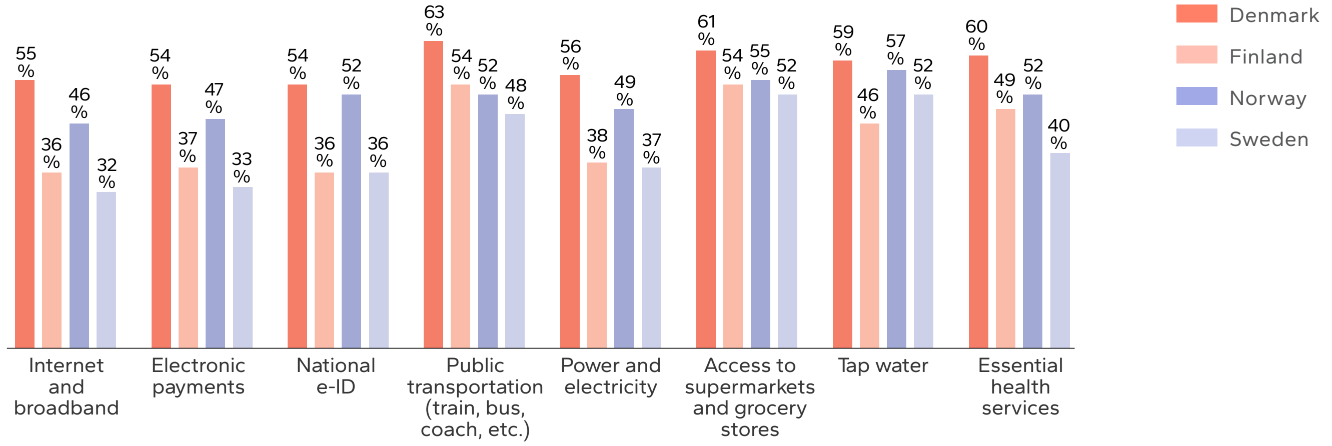
DNV Cyber's Wahlstrøm refers to storm Amy in October 2025 and the effect on the south cost of Norway, with power cut off for several days[xxi], and to the "Iberian Blackout" in April 2025 that led to a power failure across the Peninsula and brought to light critical challenges in crisis coordination and society preparedness.[xxii] While these incidents were not caused by a cyber-attack, a targeted cyber-attack on the power sector could have the same or even greater impact.

"A cyber-attack on the power sector will likely be more sophisticated and more difficult to manage than storms or technical issues within the electricity grid," says Wahlstrøm. "We currently have redundancy in both power production and distribution in most places in Norway, but we should anticipate that following a coordinated cyber-attack on the power sector, it could take more than a couple of days to recover."



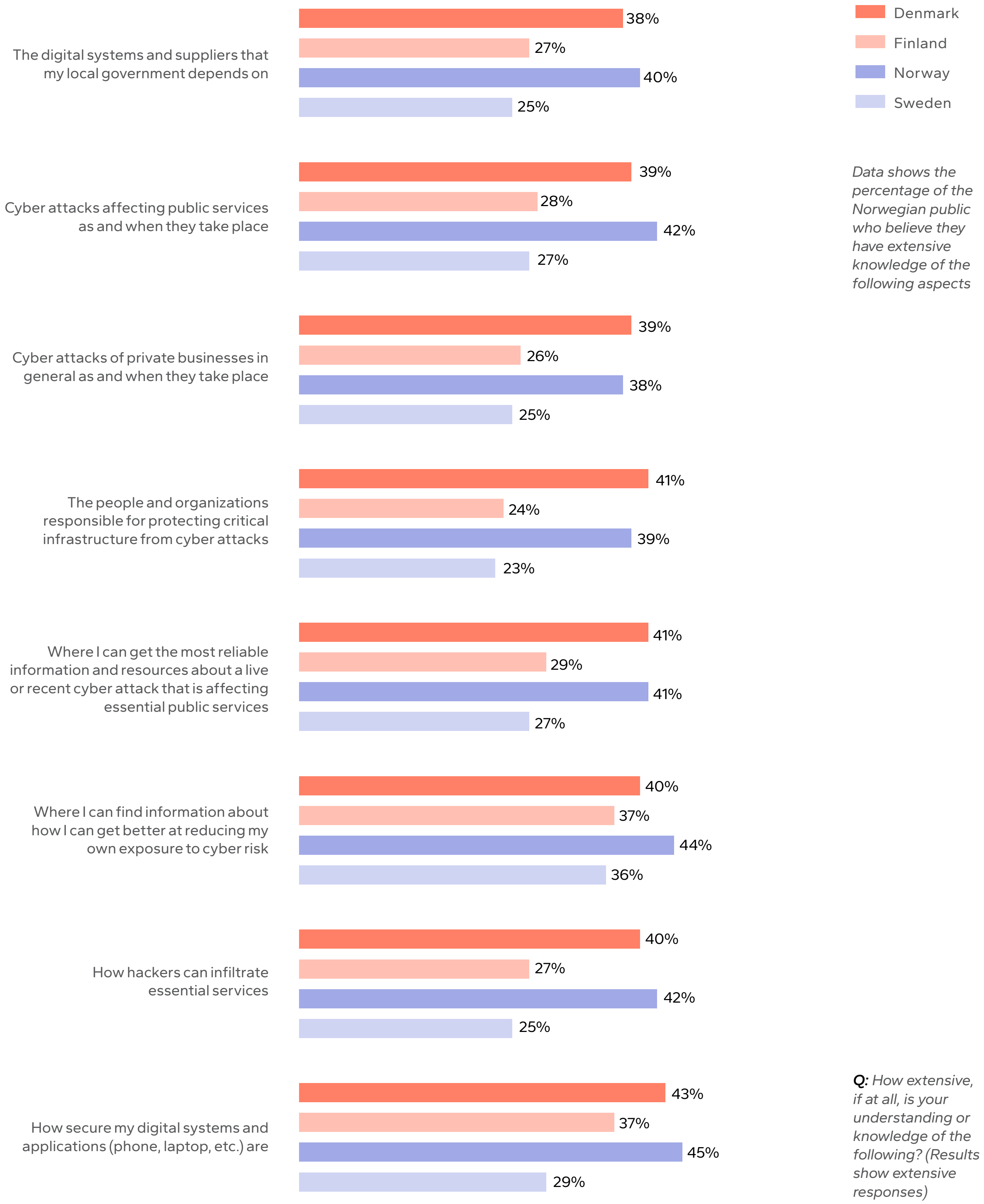
think companies should be able to fully restore their systems within a few hours after a major cyber-attack has taken place.

Norwegians are confident they would cope well in the event of a major disabling attack



***Q:** If the following resources and networks became unavailable, across the country, for a period of at least 48 hours, how confident would you be that you could make alternative arrangements and find what you needed to carry on life as normal? (Results show confident responses)*

Norwegian citizens believe they have a good understanding of critical infrastructure cyber resilience



Data shows the percentage of the Norwegian public who believe they have extensive knowledge of the following aspects

***Q:** How extensive, if at all, is your understanding or knowledge of the following? (Results show extensive responses)*

6. COLLABORATE ACTIVELY AND WIDELY TO INCREASE OVERALL CYBER RESILIENCE

Closer working across every critical infrastructure sector will improve collective security.

The whole is greater than the sum of its parts when it comes to cyber resilience. When organizations work together to protect themselves, they reduce the overall risk more effectively than a business could achieve by acting alone.

One in five (19%) of critical infrastructure executives say their organization does not consider national security and its impact on society when managing their organization's cybersecurity.

Executives must recognize that the risk is not just to their own organizations: in an increasingly connected and interdependent environment, any breach of their defences has implications for many other businesses, as well as for the whole of society.

Norwegian businesses must commit to closer collaboration across critical infrastructure sectors to improve the country's overall resilience. Compared with other Nordic countries in our research, Norway marginally lags other the others in terms of how organizations in the same industries work together. They are less likely to conduct joint cybersecurity exercises and to share cybersecurity responsibility.

Collaborate for protection

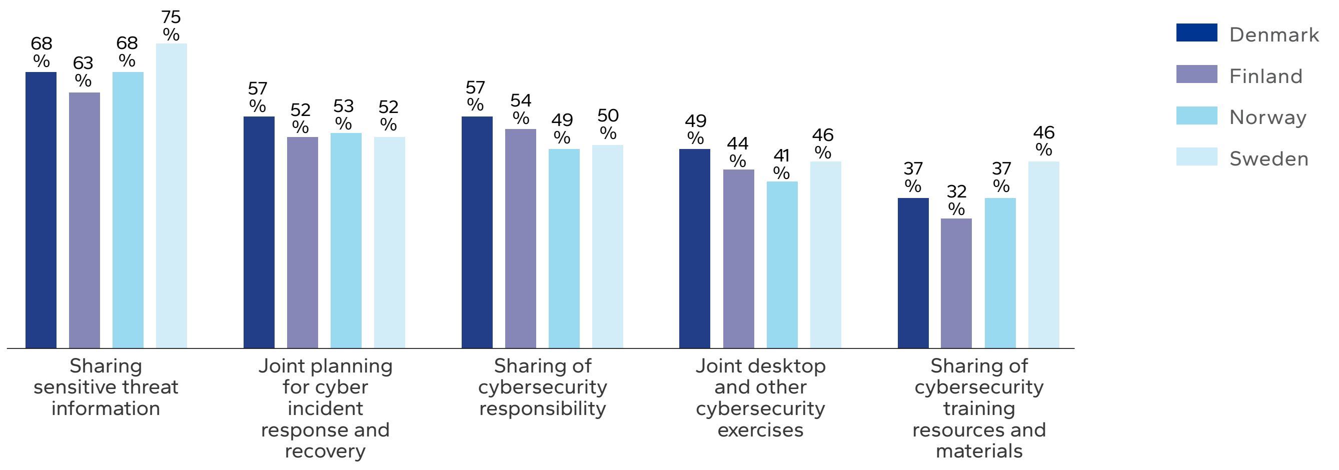
Individual organizations should seek to form alliances and partnerships, to plan jointly for critical incidents, to share information, and to train, monitor, and test together.

“Collaboration works best when there is a defined structure for information sharing and a clear mandate,” says Malmedal. “That allows information to flow more freely.” The Norwegian Business and Industry Security Council, says Malmedal, is building a platform where members can share insights and intelligence via a secure portal with agreed standards around encryption.

Industry associations and trade bodies could play a critical role as convenors of these partnerships. Organizations such as the Norwegian Directorate for Civil Protection, which already works with partners such as the National Security Authority and NorCERT on threat analysis, risk management, and incident planning, could also increase cross-party and sector exercises. Such exercises are already under way. In late 2025, Norway conducted its largest-ever national digital security exercise, with 60 participants from various sectors, including government agencies, the armed forces, and private enterprises.

The Nordic Cyber Healthcare Forum, led by DNV, is another collaborative example, providing a platform for representatives from healthcare organizations across the Nordics to discuss challenges and exchange best practices to strengthen cybersecurity in healthcare[xxiii].

Critical infrastructure organizations in Norway are marginally less likely to share cybersecurity responsibilities with industry peers



***Q:** What would you say is your organization's level of collaboration with other organizations in your industry (including suppliers, competitors and government agencies) when it comes to the following initiative? (Results show consistent responses)*

7. REVIEW HOW REGULATION CAN HAVE THE BIGGEST IMPACT ON RESILIENCE

Cyber regulation is strong in Norway, but government and business must work more closely together to ensure that required standards are achievable.

Forty-one percent of critical infrastructure executives in Norway believe that well-designed and effective regulation has made a material improvement to the cyber resilience of Norway's critical infrastructure. And 40% say the same about the adoption and enforcement of this regulation.

There is a problem. While in our research, Norwegian executives are more likely than executives in other Nordic countries to say that the regulatory environment is a source of progress, many are struggling to adapt to regulatory change. Only half (52%) say their businesses are well-prepared for keeping up with new regulations.

“It's a jungle out there,” says the National Security Authority's Albert-Hoff. “It requires serious effort for organizations, particularly smaller ones, to figure out what regulation applies to them and how they can be compliant. Norway is in a strong regulatory position due to its longstanding National Security Act, but the government could do more to ensure regulations are as easy as possible to understand and comply with.”

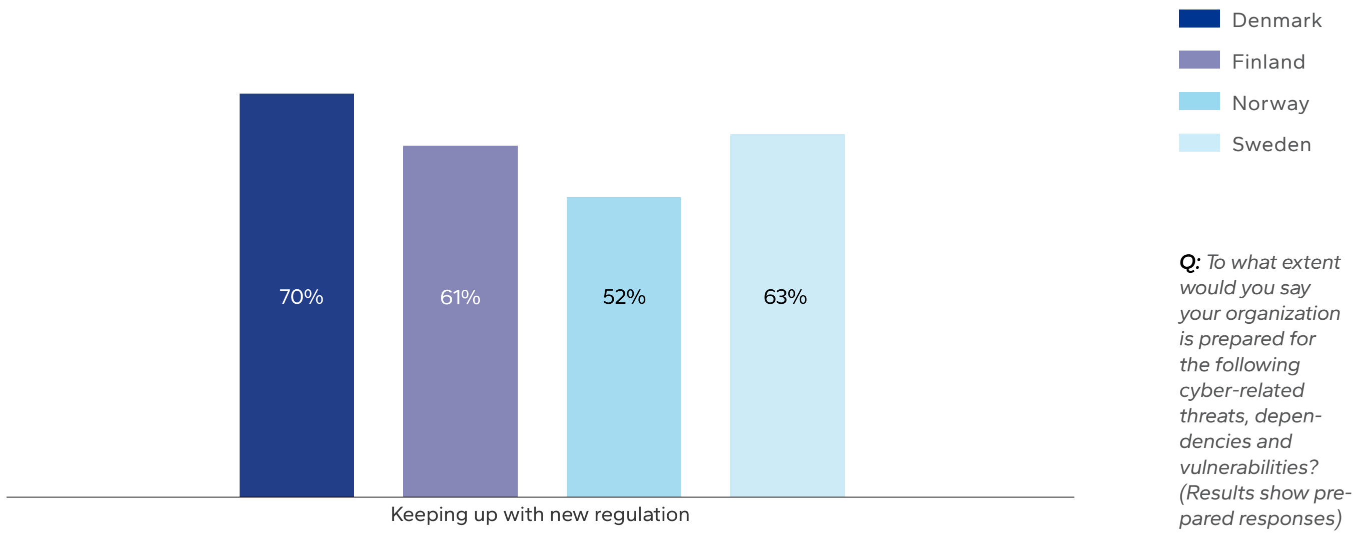
Clarify expectations

There is little point in regulation that organizations cannot comply with. While regulation needs to evolve along with the rising threat to critical infrastructure, Norwegian authorities must be proportionate and mindful that organizations understand what is required of them. Nearly three-quarters of executives say more clarity is needed from government authorities about the role that their organization is expected to play in supporting national cyber resilience.

To achieve this, it is important that regulation focuses on outcomes rather than being rule-based. “It's less about being prescriptive about how companies should manage their risks, and more about having a process to identify risks and take mitigating actions. Key to this is identifying potentially overlapping regulatory demands, to find opportunities to tackle these demands together as part of strengthening cyber resilience,” says DNV's Bartnes. “Doing this might require a shift in mindset: it is easy to fall into the trap of seeing regulation as a compliance exercise in box-ticking, rather than something that will help secure your organization.”

52% *say their businesses are well-prepared for keeping up with new regulations.*

Norwegian organizations are the least likely to say they are prepared for emerging cyber ecurity regulation



***Q:** To what extent would you say your organization is prepared for the following cyber-related threats, dependencies and vulnerabilities? (Results show prepared responses)*

CONCLUSION

What secured us yesterday won’t secure us tomorrow

Norwegian critical infrastructure organizations can’t rest on their laurels.

Our research finds that a majority of Norwegian executives working in industries deemed most critical to the running of society are confident about the cyber resilience of their organization and Norwegian critical infrastructure. But the leading driver of this confidence is past success in quickly responding to attacks, coming ahead of factors such as training that address the next generation of cybersecurity risks.

Cyber-attacks are increasing and threats are becoming more sophisticated – such as with attackers targeting vulnerabilities in supply chains and bolstering attacks using AI. Taking confidence from previous security measures can be dangerous.

“Norway may not have experienced as many successful attacks on our critical infrastructure as our Nordic neighbours – counting those that have been disclosed publicly – but past successes do not guarantee future resilience,” says DNV Cyber’s Kalleklev.

> *With geopolitical tensions rising and attackers becoming increasing sophisticated, the threat to our critical infrastructure is fundamentally different to the past.”*
>
> *Arve Johan Kalleklev, Operations Director at DNV Cyber.*

Norway is making progress towards cyber resilience, but many questions remain. Is the current regulation driving real resilience or just pushing businesses into compliance, and what more can the authorities do to stimulate positive change? How will countries measure progress to ensure that public-private initiatives are having the desired effect? And how can businesses and the public make sure they are doing all they can, with all the tools and knowledge available to them, to achieve an acceptable baseline of preparedness?

There are no easy answers. Above all, however, resilience must now be treated as a shared national priority, led by government but involving business and the public every step of the way. Our expectation is that cyber resilience will only be achieved through a substantial, coordinated approach providing sharper guidance, outcome-focused regulation and incentives, more regular joint exercises across sectors, and sustained public education that builds trust across the critical infrastructure system.

In an interconnected system, which relies on digitalization to unlock further efficiencies and innovation in how services are delivered, this is the way forward. But no single country or industry has developed an approach that guarantees resilience in a rapidly evolving threat environment. An iterative approach, based on knowledge-sharing across international borders, is essential.

REFERENCES

1 Huge aluminium plants hit by 'severe' ransomware attack, *BBC*

2 Hacked, but not cracked: From cyberattack to resilience, *Onitio*

3 Spy ships, cyber-attacks and shadow fleets: the crack security team braced for trouble at sea, *The Guardian*

4 Financially motivated cyber crime remains biggest threat source, *ComputerWeekly*

5 Threat and risk assessments 2026, *Norwegian authorities*

6 Norway Activity Report, *Radware*

7 Norwegian Refugee Council hit by cyberattack, *The Record*

8 Nordic Financial, *Cert*

9 Security Act, *Lovdata*

10 Veiledning til kraftberedskapsforskriften, *Norwegian Water Resources and Energy Directorate (NVE)*

11 National Cyber Security Strategy for Norway, *Norwegian Government*

12 Norway's Digital Security Act - Now in effect, *Schjodt*

13 Totalberedskapsmeldingen, *Regjeringen, Justis- og Beredskapsdepartementet*

14 Digitalsikkerhetsloven trådte i kraft 1. oktober 2025, hva betyr det for virksomheter? *Sicra*

15 Who or what has access to what? *DNV Cyber*

16 CERT Polska details cyberattacks on Polish manufacturer, energy sites; fails to disrupt power and heat supply, *Industrial Cyber*

17 Energy Transition Outlook, 2025, *DNV*

18 New report: Solar sector proposes solutions to mitigate critical cybersecurity risks, *SolarPower Europe*

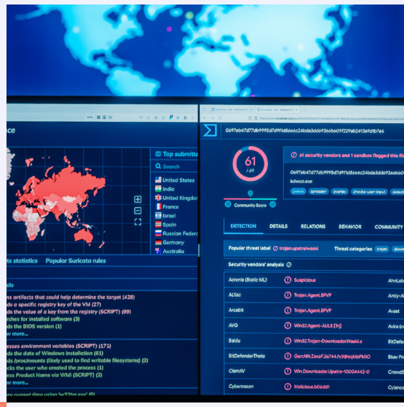
19 Russia’s Shadow War Against the West, *CSIS*

20 How Low Can You Go? An Analysis of 2023 Time-to-Exploit Trend, *Casey Charrier, Robert Weiner*

21 Ny mørk natt for tusenvis av kunder, *TV2*

22 Beyond the Blackout - Cybersecurity insights from the Iberian power outage, *DNV Cyber*

23 Nordic Cyber Healthcare Forum builds cyber resilience, *DNV Cyber*



Images: DNV Cyber; page 35. GettyImages; pages 2, 6, 13, 16, 22, 23, 25, 29. Shutterstock; pages 1, 2, 8, 16, 18, 20, 26, 30, 34. Unsplash; 1, 20.

DNV
CYBER

About DNV Cyber
DNV Cyber is a leading cybersecurity services provider. We empower businesses with complex needs to become safer and more resilient with tailored solutions. Our global team of more than 500 experts brings over 30 years of IT and industrial control system security experience to your business, helping you breathe easier and perform better.

We identify, prioritize, and communicate risk, guide you through regulations, and align your cybersecurity with your business goals. We bring you technology and threat insight, help you to secure cyber investments, and implement cost-effective security control measures. We detect and respond to threats, ensuring continuous improvement and quick recovery.

We ask questions and listen, speaking your industry's language. We collaborate and share insights, setting industry standards and delivering best practice. We safeguard your critical, enabling your business to thrive.

DNV Cyber was formed by merging Nixu, Applied Risk and DNV in 2024.

About DNV
DNV is an independent assurance and risk management provider, operating in more than 100 countries, with the purpose of safeguarding life, property, and the environment. As a trusted voice for many of the world's most successful organizations, we help seize opportunities and tackle the risks arising from global transformations. We use our broad experience and deep expertise to advance safety and sustainable performance, set industry standards, and inspire and invent solutions.

> *DNV Cyber safeguards your critical.*

Disclaimer. All information is correct to the best of our knowledge. Contributions by external authors do not necessarily reflect the views of the editors and DNV.