



**Security that goes  
beyond technology  
to empower societies**

---

telenor



# Contents

Introduction	<b>3</b>
What are business leaders telling us?	<b>7</b>
Blurred lines: the complexity of living in a post-truth world	<b>9</b>
Finding answers	<b>12</b>
Security by design: development of 5G	<b>13</b>
Detection, analysis and response: a service approach	<b>15</b>
Industrial cybersecurity: bridging the real and the digital with Omny	<b>15</b>
Strength in unity: the value of Nordic cooperation	<b>16</b>
Raising awareness: people are the last line of defence	<b>19</b>
Conclusion	<b>22</b>



## INTRODUCTION

# Greater data, greater complexity, greater uncertainty

In an ever more complex and digital world, organisations, leaders and individuals must be able to handle uncertainty – by leveraging technology, strengthening collaboration, building awareness, overcoming fear and sharing responsibility.

The pace of digitalisation is increasing drastically. For instance, there were seven billion IoT (Internet of Things) units in 2018. In 2025, according to Statista estimates, there will be more than 75 billion. Devices from thermostats and electric meters to cars and streetlights will be interconnected. This growing dependency on digital systems – intensified by COVID-19 – has altered societies.

Rapid digitalisation risks exposing economies to new and more intense cyber vulnerabilities, as new technologies and an ever-expanding attack surface create greater opportunity and lower the threshold for cybercrimes.

Alongside this rapid digitalisation, the war in Ukraine began in February 2022. As a consequence, Europe is experiencing increased geopolitical tension and economic fragmentation, especially for trade and technology.

Furthermore, this conflict is leading to increased cyberthreats. According to a 2023 report by Google's Threat Analysis Group (TAG), Mandiant and Trust & Safety, Russian government-backed attackers ramped up cyber operations beginning in 2021. In 2022, Russia increased targeting of users in Ukraine by 250% compared to 2020, while targeting of users in NATO countries increased over 300% in the same period.

The report explains that the attackers focus heavily on Ukrainian government and military entities, but also show a strong focus on critical infrastructure, utilities and public services, and the media and information space. And this is not just in Ukraine; recent years have seen attacks on the wider financial, health and energy sectors – underlining that cybercrime doesn't only impact large companies (see box on page 6), but can disrupt functions that are critical to society and therefore the everyday lives of individuals.

At Telenor, we know that connectivity is more important than ever. But now we also see that the market demands solutions that go beyond connectivity – services on top, such as security. Digital security has never been as critical as it is today, and it is becoming more so day by day. The world is at a cyber crossroads – and it is up to everyone to step up in the search for responses.

### **What role can telecommunications companies play?**

The expectations towards telecommunications companies to take responsibility securing their customers and society is very high. This is one of the findings of an April 2023 survey of over 2,000 business leaders in the Nordics, carried out for Telenor by leading data collector Norstat.

The full details can be found in the text below. In general, leaders rated telcos second, only behind cybersecurity providers, when asked to what degree they expect institutions and industries to take responsibility for protecting businesses and society at large against cyberattacks.

This therefore puts telcos above government agencies and financial and educational institutions in terms of their responsibility towards society. It also highlights the perception of telcos as playing a role that goes beyond being a provider of technology (as important as that role is) to being a trusted protector of critical infrastructure and functions.

At Telenor, we live up to these expectations. As proved during the pandemic, as well as in everyday life, we provide robust networks, ensure continuity of connectivity and protect critical infrastructure. We develop cutting-edge technology that is secure by design and we offer detection and response services that our customers can rely on. We invest more than USD 1 million annually in security infrastructure and averting threats.

Our actions underline how advanced technology can support and empower societies. But we go beyond being a tech and infrastructure provider. We are a collaborator, working together with other companies, with governmental authorities and with communities – because we know that the threat landscape is too complex to handle alone. And we raise awareness and educate our customers, leaders and employees to understand the threats and take control of their digital security. We're protecting multiple stakeholders, advancing the digital world while making it safer for all.

# The bigger picture

Global mobile data traffic (excluding fixed wireless) exceeded

## 49 exabytes

(that's 49 billion gigabytes) per month at the end of 2020 – and the monthly total is set to hit 237 exabytes in 2026.

Figures from Ericsson and Thales.

The annual cost of cybercrime to the global economy is estimated to have reached

## EUR 5.5 trillion

at the end of 2020, double the figure of 2015.

EU Agency for Cybersecurity.

From its incident response work, Mandiant observed more destructive cyberattacks in Ukraine during the first

## 4 months

of 2022 than in the previous 8 years with attacks peaking around the start of the invasion.

Google TAG report *Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape*.

In Norway, from 2019 to 2021, there was a

## tripling in serious cyber operations

against Norwegian authorities and businesses.

*Risiko 2023* report published by the Norwegian National Security Authority/NSM.

In February 2022 alone, Telenor's security centre TSOC detected

## 67 potentially

serious security incidents.

Figure from Telenor.

## Nearly 6 out of 10 people

(57 percent) are concerned that cyberattacks will disrupt functions that are critical to society.

Figure from the April 2023 survey of 4,000 people in Denmark, Finland, Norway and Sweden carried out by Norstat for Telenor.

Link:

More info on this survey and cybersecurity challenges can be found on Telenor's ListenUp! platform.

<https://www.telenor.com/listen-up/>



## What are some of the costliest cyberattacks of all time?

- 1 EPSILON: USD 400 MILLION.** In 2011 Epsilon, a major email marketing company with clients such as JP Morgan and Target, had its lists of thousands of customers' names and email addresses stolen, ultimately paying large sums in fines and compensation claims.
- 2 MAERSK: USD 300 MILLION.** Although not the original target, shipping giant Maersk's systems were infected by the encryption virus NotPetya in 2017. They rebuilt their entire IT system in just 10 days, but in that time they lost millions of dollars.
- 3 HANNAFORD BROS: USD 252 MILLION.** In 2007, the Hannaford grocery chain was attacked by a Russian/Ukrainian hacker group that stole the credit card information of 4.2 million customers, and at least 1,800 of these were used by the hackers.
- 4 US DEPARTMENT OF VETERANS AFFAIRS: USD 100-500 MILLION.** The department had not encrypted info for 26.5 million veterans and their families, which was also saved on an external laptop and USB. In 2006, the entire list of names and information was stolen by hackers, leading to large compensation claims and fines.
- 5 NORSK HYDRO: USD 70 MILLION.** The LockerGoga virus infected this renewable energy and aluminium company's systems for 2-3 weeks before it was discovered. The attack involved locking all systems (22,000 PCs were affected) and demanding a ransom to open them again.

# What are business leaders telling us?

As mentioned above, Telenor conducted a survey with Norstat in April 2023 to explore business leaders' experiences and perspectives towards cybersecurity.

A total of

**2,162**  
business leaders

in the Nordics were surveyed, making this the most extensive survey of its kind.

**One in five**  
leaders

say their company has experienced a cybersecurity incident or attack in the past year.

There is a high level of awareness and concern in all markets.

**95** percent

of all business leaders say they are aware of cybersecurity threats to their business and one in four state that they are extremely aware. Three in four are concerned that their business could be put out of operation due to a cybersecurity attack.

More than half of the companies surveyed say they will invest more in cybersecurity in the future –

**53** percent

say this is very likely or somewhat likely. Currently, 92 percent of respondents allocate 25 percent or less of their business's resources to cybersecurity measures.

**Lack of knowledge and expertise**

is the largest obstacle to improving cybersecurity, followed by lack of understanding and awareness among employees – underlining that it's not just technology, but also people who have a strong role to play in combatting cyberthreats.

## What are the most commonly used attack techniques

- **MALWARE:**  
This term describes malicious software, including spy-ware, ransomware, viruses and worms. Malware breaches a network through a vulnerability, typically when a user clicks a dangerous link or email attachment that then installs risky software.
- **PHISHING:**  
This is the practice of sending fraudulent communications that appear to come from a reputable source, usually through email. The goal is to steal sensitive data like credit card and login information or to install malware on the victim's machine.
- **MAN-IN-THE-MIDDLE ATTACKS:**  
Also known as eavesdropping attacks, these occur when attackers insert themselves into a two-party transaction. Once the attackers interrupt the traffic, they can filter and steal data.
- **DENIAL-OF-SERVICE ATTACK:**  
This type of attack floods systems, servers or networks with traffic to exhaust resources and bandwidth. As a result, the system is unable to fulfil legitimate requests.
- **SQL INJECTION:**  
A Structured Query Language (SQL) injection occurs when an attacker inserts malicious code into a server that uses SQL and forces the server to reveal information it normally would not. An attacker could carry out an SQL injection simply by submitting malicious code into a vulnerable website search box.
- **ZERO-DAY EXPLOIT:**  
A zero-day exploit hits after a network vulnerability is announced but before a patch or solution is implemented. Attackers target the disclosed vulnerability during this window of time. There are also N-day attacks, which are more frequent. They exploit known vulnerabilities, for many of which a patch or other remedial measure has been known and available for significant periods of time.
- **DNS TUNNELLING:**  
This uses the DNS protocol to communicate non-DNS traffic over port 53. It sends HTTP and other protocol traffic over DNS. There are various, legitimate reasons to use DNS tunnelling. However, there are also malicious reasons to use DNS Tunnelling VPN services. They can be used to disguise outbound traffic as DNS, concealing data that is typically shared through an internet connection. For malicious use, DNS requests are manipulated to exfiltrate data from a compromised system to the attacker's infrastructure. It can also be used for command and control callbacks from the attacker's infrastructure to a compromised system.

All info from Cisco:

[Cyber Attack - What Are Common Cyberthreats?](#)



# Blurred lines: the complexity of living in a post-truth world

What makes the current situation even more complex are the increasingly blurred lines between perpetrators: who are the real criminals and are they even human – or are they actually AI?

To start with, the hacker community itself isn't homogenous, with white-hat hackers on one side and cybercriminals on the other. These criminals operate within very different types of organisation, ranging from well-organised state actors to kids in their bedroom – who are often interested in monetary gains – as well as hacktivists, who are acting for political reasons. And whereas cybercrime used to be more about individuals or gangs, it is now becoming more like an industry with large criminal organisations consisting of departments, rather resembling a corporation.

Furthermore, the model of how cybercrime is perpetrated is multi-layered: for example, some people write malicious code, other actors buy the code from them, and a third actor is hired to carry out the attack. Crime-as-a-service (see box), which is a new development, works along similar lines.

All this leads to the question: who is the criminal – is someone selling a technical capability for a fixed price merely a service provider or a real perpetrator of crime? Whatever the definition of criminal, this new set-up makes it easier for more people to be able to commit crimes.

## What is crime-as-a-service?

A new development, crime-as-a-service is a way for non-technical cybercriminals to access sophisticated tools without having the competencies to develop such tools themselves. In other words, they 'buy' the services in. Crime-as-a-service is like other technology development business models. The cybercriminal develops

the technology that can then be sold or rented to multiple customers, and the customers, who are criminals, benefit from the use of such technology to run their business, in the same way that legitimate businesses leverage technology. Ultimately, through crime-as-a-service, the barrier for entry into cybercrime is lowering.

Another technology that is increasing the threat level is AI (artificial intelligence), which makes it more difficult to judge whether information that people receive is real or not. For example, it's now possible to recreate a person's voice from just a three-second sample. This means that someone could receive a call from their child asking them to transfer money in a supposed emergency, but the call is actually from a criminal.

In the future, AI may be able to scan social media profiles, detecting articles that a potential victim likes, comments they leave and what they are interested in; it could then tailor a message so perfectly that it will be very difficult for a victim to ascertain that the message isn't real. This means that

how a perpetrator conducts an attack will change and protecting victims will be more challenging.

Questioning and critical thinking is required when faced with such phishing attempts. This could also apply to AI-based chatbots like ChatGPT, which looks very believable but is also known to have uneven factual accuracy and it's not clear what sources it draws on (see next page for more on the dangers of generative AI). If humans become caught in a self-perpetuating cycle of AI-generated facts being recapitulated in other sources, ascertaining what is real and what is fake news, and helping individuals feel more certain navigating the digital world, become major challenges for all.



# What is generative AI and what dangers does it pose?

This is what ChatGPT had to say:

Generative AI refers to a class of artificial intelligence models and techniques that are designed to generate new content, such as images, text, music, or even videos, that is similar to existing data it has been trained on. These models are typically trained using large datasets and employ deep learning algorithms, such as generative adversarial networks (GANs) or autoregressive models.

Generative AI has shown remarkable advancements in various fields and has applications in creative industries, data synthesis and content generation. It can produce realistic images, generate human-like text, compose music and much more. It has the potential to revolutionise areas like art, entertainment, design and automation.

**However, generative AI also poses certain dangers and ethical concerns. Here are a few key considerations:**

## **1. MISUSE OF GENERATED CONTENT:**

Generative AI can be exploited to create realistic but fake content, such as deepfake videos or synthetic personas, which can be used for malicious purposes like disinformation, impersonation or fraud.

## **2. PRIVACY CONCERNS:**

Generative AI models are often trained on large datasets, which can include personal information. If not handled properly, these models may inadvertently reveal sensitive or private data about individuals.

## **3. AMPLIFICATION OF BIASES:**

If the training data used for generative AI contains biases, the models can learn and perpetuate those biases in the generated content, leading to unfair or discriminatory outcomes.

## **4. INTELLECTUAL PROPERTY INFRINGEMENT:**

Generative AI models can produce content that resembles existing copyrighted works, potentially raising legal issues regarding intellectual property rights.

## **5. PSYCHOLOGICAL IMPACT:**

The creation of highly realistic and manipulative content by generative AI can have psychological consequences, such as causing confusion, eroding trust or manipulating public opinion.

## **6. SECURITY RISKS:**

Generative AI models can also be targeted and manipulated by malicious actors. Adversarial attacks can be used to exploit vulnerabilities in the models, potentially leading to the generation of harmful or misleading content.

Addressing these dangers requires a combination of technical solutions, regulatory frameworks and ethical guidelines. Ongoing research and responsible development of generative AI, along with robust safeguards and awareness, are crucial for mitigating these risks and ensuring the responsible deployment of this technology.

[Accessed on 22 May 2023 using the Free Research Preview version of ChatGPT]



# Finding answers

***But if the security situation is becoming ever more challenging, where are the answers to be found?***

It takes a combination of state-of-the-art technology, collaborative projects across multiple stakeholders, and empowering people to feel confident in navigating the online world.

**Here are some highlight projects in which Telenor is involved.**

## Security by design: development of 5G

The new fifth generation (5G) of mobile connectivity is known for hyper-fast download speeds, low latency and the capability to really unlock the full potential of the smart world ever more people live in. 5G supports a variety of verticals, such as the Industrial Internet of Things, and the automotive, transport and healthcare sectors – and will accommodate new services and applications such as augmented reality and seamless streaming to all. In this sense, it's less about being bigger and faster, and more about enabling a new set of services that will change many aspects of everyday life.

Another change: the number of connected and managed devices will be by orders of magnitude higher than with 4G Long-Term Evolution (LTE). This has an implication for security as an increase in connected devices creates more targets and larger attack surfaces. Furthermore, 5G's use of the cloud and edge computing, and convergence of mobile and traditional IT networks, create new attack vectors. And 5G introduces the concept of network slicing to logically divide virtual networks, which

also obscures potential vulnerabilities.

Although security in 5G is much more improved compared to 4G, 3G and 2G, the above examples demonstrate that there are new security challenges. But just as technology brings challenges, it also brings hope – and Telenor has been exploring the use of AI as one possible provider of solutions.

For example, AI can monitor network performance and detect anomalies that could indicate security breaches or malicious activities. By analysing network control and management traffic, AI algorithms can identify unusual patterns, such as unexpected changes in network behaviour, which may indicate a security threat. Similarly, by identifying patterns and trends, AI models can predict potential security risks and proactively take measures to prevent them.

AI is also playing a role in building more secure authentication systems. Through behavioural biometrics, facial and voice recognition, analysing user behaviour data and identifying anomalies, AI can add new levels of security to traditional authentication methods.



## Part of CONCORDIA project to strengthen European cybersecurity

As cybersecurity is too big a challenge to handle alone, Telenor has been contributing to the CONCORDIA research and innovation project, which ended on 31 March 2023. With funding from the European Union's Horizon 2020 programme, CONCORDIA has delivered 21 outcomes and over 300 scientific publications, while creating a multi-stakeholder ecosystem comprising over 50 stakeholders from research, industry, start-ups and public bodies. The four-year project covered a wide range of topics, including cyberattacks on critical infrastructure, information security and data protection, certification and competence building.

Telenor contributed to these outcomes, developing a cyberthreat intelligence platform for the telco sector. Overall, this pilot involved analysing attack types targeting this sector, collecting and sharing information about them, and

protecting users and organisations from malicious cyberattacks. It worked on three use cases, with several benefits coming from each case, such as zero-day attack detection or detecting privacy violations on users' data.

Project coordinator Professor Gabi Dreo from the University of the Bundeswehr Munich summarised: "CONCORDIA's results will not only provide valuable input to the European Cybersecurity Competence Centre and the network of National Cybersecurity Centres, and with this to the whole European cybersecurity community, but they will also work to strengthen and speed up research, development, and especially innovation."

More info on the telecom sector pilot project can be found [here](#).

## DETECTION, ANALYSIS AND RESPONSE: a service approach

Network traffic analysis and anomaly detection isn't something that Telenor only uses to keep its own infrastructure more secure; we use our advanced technology and cutting-edge security expertise to potentially prevent cyberattacks on our customers' systems, too.

IDS (Intrusion Detection System) Security Monitoring is a fundamental NDR (Network Detection and Response) service provided by the Telenor Security Operations Center (TSOC). The process involves identifying critical points in the customer's internal network and strategically placing IDS sensors. These sensors passively listen, analyse and detect any abnormal activity without impacting network traffic. Detected incidents are transmitted to the security centre for closer follow-up. If automated analysis is inconclusive, the incidents are forwarded to experts for further examination, classified based on severity and the customer is notified accordingly.

The expertise of the TSOC security experts enables the detection of cyberattacks that fully automated security solutions might overlook. The fact that TSOC is manned around the clock means that attacks can be detected at a very early stage, minimising potential damage. However, attackers are skilled at finding alternative routes into systems, making it necessary to secure multiple areas. Many sources of infection and attacks cannot be captured through the customer's broadband access. Additionally, encrypted internet traffic and the mobility of devices pose challenges for security monitoring.

To address these challenges, TSOC offers its Log Analysis service as a crucial component of company security. Log Analysis allows for the detection of abnormal login attempts and provides a more comprehensive view of network security. Log data from critical IT equipment, such as routers, firewalls and servers, is continuously collected and analysed by

TSOC. Often, businesses fail to follow up on this data, potentially missing serious incidents. By analysing log data, TSOC can detect patterns, compare them with known attack techniques and classify incidents based on severity.

To further enhance our security offering, Telenor offers the Active Response service. This service goes beyond monitoring and response, allowing TSOC to take action on behalf of the customer. Previously, the customer's IT environment had to handle incident response, such as isolating infected PCs – and with Active Response, TSOC can perform this action.

### Links:

More info on this portfolio (in Norwegian) can be found here:

[Sikkerhetsovervåkning/Security Monitoring - IDS](#)

[Logganalyse / Log Analysis](#)

[Aktiv Respons / Active Response](#)

## INDUSTRIAL CYBERSECURITY: bridging the real and the digital with Omny

With the increased adoption of cloud technologies, industrial companies are looking to achieve improved efficiencies and remote monitoring capabilities for their operational technology (OT) systems. While this connectivity brings benefits like improved efficiency and remote monitoring, it also expands the attack surface and exposes industrial control systems to cyber threats. Simultaneously, cybercriminals have recognised the potential impact of disrupting industrial operations.

As a timely response to this situation, Omny was founded in 2022 by Telenor, Aker Group (one of the biggest industrial groups in Norway) and Cognite (a global industrial DataOps platform provider). This cooperation draws on Telenor's cybersecurity capabilities and Cognite's

expertise in analysing operations-related data and how this impacts real-world scenarios, such as making production in smart factories more efficient – in other words, bridging the IT and OT spheres.

Omny offers digital representations of a customer's cyber-physical environment – in order to calculate digital risks, assess the threat landscape, detect unwanted behaviour and ascertain the impact on their operations. Omny reveals cybersecurity risks in the context of the most important physical and digital assets, processes and systems. It also shows how a cyberattack on one of the components in an industrial company's infrastructure can affect key processes and production.

This offering takes the network monitoring role of a Security Operations Centre (SOC) a step further, adding in an understanding of the gravity within real-world scenarios – which is a unique proposition. As an example: a SOC is monitoring a section of railway track, filtering alerts and their related IP addresses. Alerts are often assigned severity levels based on the potential impact of the incident – and this level can be determined by the criticality of the affected system or infrastructure, and the potential consequences of a successful breach. Here, real-world knowledge is crucial: there is a major difference between a storeroom door being accidentally locked and a light malfunctioning in a railway signal along a busy track.

Omny's portfolio therefore enables C-suite leaders to fully understand the risk in terms of impact on business, allowing them to make more accurate and quicker decisions, both on a strategic and tactical level. This decision-making capability helps business leaders and cyber experts within an organisation 'speak the same language' – bridging potential leadership divides, alongside the gap between IT and OT and between the real and digital worlds.

The WEF's **Global Cybersecurity Outlook 2023** report states: cyber and business leaders still have a great deal of work to do to truly understand each other, articulate the risk cyber issues pose to their business and translate that into meaningful management and mitigation measures. It also points out that as the cyber landscape becomes more complex, it is critical that organisations work to resolve this now if they are to build long-term cyber resilience.

Alongside supporting these goals, the insight that Omny offers also addresses the issue of lack of knowledge and expertise that was revealed by the April 2023 business leader survey. It found that a lack of knowledge and expertise is the most important obstacle for improving cybersecurity. While technological advances are invaluable in the race to combat cyberthreats, supporting the way that people interact, learn and respond is equally important.

#### Link:

The WEF's Global Cybersecurity Outlook 2023 can be found [here](#).

### **STRENGTH IN UNITY: the value of Nordic cooperation**

In response to increased cyberthreats, several governments have implemented stricter security laws and regulations. This has, in turn, led Nordic countries to implement regulations that differ across markets, creating regulatory and legal fragmentation.

What are the consequences of this? In short, a fragmented landscape hinders cross-border collaboration between cyber defence experts. In addition, national procedures for security clearances are



cumbersome and demand is increasing faster than supply. This limits the ability of Norwegian personnel with security clearance to work in Sweden to protect Swedish networks and vice versa.

Furthermore, a fragmented approach limits the possibilities of building effective, redundant networks across borders. When war broke out in Ukraine, one of the solutions operators used was to increase international cross-border cooperation. Considering a hypothetical situation: if parts of Denmark, Finland, Norway or Sweden were physically attacked along with their networks, it would be advantageous to have a structure in place that enables backup data to be stored and traffic to be routed through neighbouring countries.

Cooperation, therefore, is about being able to lean on each other in times of crisis and conflict – with mutual dependencies leading to greater robustness. Strength comes

from building security together. However, there is currently a lack of collaboration between the Nordic countries on infrastructure and cybersecurity, including leading telecommunications operators.

Establishing cross-border collaboration between authorities and private telcos, and pooling competencies, is key. Companies need to work closer with governments and authorities across borders in the fight against cyberthreats – and to remove obstacles to effective collaboration between public and private sectors. As a pan-Nordic operator, Telenor has experience working with governments in all Nordic markets.

Telenor also lives up to its role of being there when society needs us – in everyday situations and in crises. We have an important part to play in creating a well-prepared and resilient society capable of withstanding a range of threats and



challenges, including military aggression, natural disasters, cyberattacks and societal disruptions. The telecoms sector plays a crucial role on multiple levels: in the military's ability to operate, in the possibilities of maintaining psychological defence and in ensuring that other vital sectors such as electricity, water and food supply can function.

The April 2023 business leader survey indicated respondents' expectations towards the role of telecommunications

companies is very high. Respondents were asked to what degree they expect institutions and industries to take responsibility to protect businesses and society at large against cyberattacks. Telcos rated second, only below cybersecurity providers. Telenor itself also rated highly against other telcos in the region in terms of taking that responsibility: it scored top three in all markets and is clearly number one in Norway.

## Outside view from Norway's National Cybercrime Centre (NC3): trust plays a role

Else Gun Ommundsen and Espen Skogstad are business liaison officers at NC3. On the topic of cooperation between the public and private sector, they explain that it is increasing and has become very good in Norway. They add that, in their experience, the trust companies and the public sector have towards law enforcement is high.

Both colleagues have seen the benefits of collaboration between authorities and companies and they urge companies to contact the authorities to prevent cybercrimes happening repeatedly. This is underlined by their experience with Norsk Hydro, the aluminium and renewable energy company that was hit by a

ransomware attack in 2019. They explain that this attack was known in other places around the world, so the information from those cases was shared and NC3 was able to notify other potential victims to check their systems.

Norsk Hydro reported their attack, and were generally praised for their openness, which arguably had a positive reputational impact. This reflects the findings of the April 2023 business leader survey. Almost 6 out of 10 business leaders believe that disclosing information about cybersecurity incidents builds trust and positive reputation, with only five percent disagreeing.

## **RAISING AWARENESS: people are the last line of defence**

While collaboration between companies and between authorities and the corporate world is crucial, it's still not enough: every colleague, leader and individual has a role to play.

When creating this culture of shared responsibility, several factors should be taken into account: it's important to realise that accessibility, openness and a no-blame culture are required to overcome lack of awareness and/or uncertainty around digital technologies and cyberthreats. With advanced technology making it increasingly difficult for people to spot what's real or not, it's unfair to look to them for blame – instead telecommunications companies can engage with them to help change behaviours and overcome the idea that cybersecurity is too technical and inaccessible.

DNA, which is part of the Telenor Group, has been conducting its Digital Lifestyles survey for several years. Its latest 2022 edition found that nearly one-third (30%) of all respondents feel that they do not have enough information about digital threats. However, people under 35 feel that they have enough information about such threats more often than older age groups.

Even though this shows that awareness is growing, it also suggests that there is room for improvement in terms of making people more conscious about cyber issues. For example, they may not be aware of what they can do to protect themselves – or in the face of large and intangible threats, they may not think there is anything they can do at all.

For its part, DNA also understands that there's still work to do to raise awareness and overcome fears. The company strives to keep its customers safe online by



providing them with basic knowledge of different scams and tips on how to improve their digital safety. The threat landscape is changing so quickly that it's very challenging to understand all the threats and what actions are required, but technology and digital security services can provide extra safety and peace of mind.

DNA also believes that telecommunications companies have a role to play; it's within the operator's responsibility to support their customers in making sure they know how to stay safe online. It carries out activities to help people become more aware and shows them that there are tools that can help them take control of their own digital security.

### Three examples of how DNA is helping people stay safe online

- **NO-HASSLE PRODUCTS:**  
DNA Digiturva is an all-in-one app that fights viruses, ensures private web browsing, manages passwords and provides immediate alerts of data breaches. It brings together the capabilities of three previous products because DNA understands more people will protect their devices and data if we make security as easy and accessible as possible.

**Link:**

More info about DNA Digiturva (in Finnish) can be found [here](#).

- **RAISING IN-HOUSE KNOWLEDGE AND CUSTOMER AWARENESS:**  
DNA is training its customer-facing staff so they can pass this knowledge on to customers and raise their awareness, too. DNA also actively provides customers with tips and tools on how to stay safe online including with emails, online platforms and social media.

- **INVOLVEMENT IN COMMUNITY INITIATIVES AND COOPERATION WITH LOCAL AUTHORITIES:**

DNA partners with HelsinkiMissio, a non-profit organisation whose aim is to ease loneliness across all age groups. Together they formed 'Digital Help' – an initiative to digitally empower older adults which is built on HelsinkiMissio's competence in the area, combined with DNA funding, devices and employee volunteers. The aim is to help older people who feel concern or uncertainty when faced with digital technology. Furthermore, DNA cooperates with local authorities in order to block phishing calls, for example, and other threats.

### Building awareness in corporate culture

The idea that a company's security culture starts with awareness and includes everyone is underlined by the WEF's **Global Cybersecurity Outlook 2023** report. It quotes cyber leaders as saying that increased employee awareness about cyberattacks is the most positive influence on an organisation's cyber-resilience approach for the next 12 months.

Reflecting a culture of shared responsibility, the WEF recommends that business units incorporate cybersecurity requirements into their key performance indicators (KPIs), after which all leaders must demand real enforcement, real consequences and real incentives to achieve the agreed-upon KPIs.

While the WEF believes that meaningful incentive structures make change happen, figures from Gartner indicate that by 2026, 50 percent of C-level executives will have performance requirements related to risk built into their employment contracts. It's a sign that cybersecurity is growing in importance outside the CISO function.

### Three examples of how Telenor makes people part of the solution

- **CREATING A POSITIVE PEOPLE**

**CULTURE:** To help leaders and employees understand the potential risks, they are offered awareness sessions, trainings and upskilling. Telenor also strives to create an open, speak-up culture where reporting can take place.

- **CONNECTING SECURITY AND**

**BUSINESS LEADERS:** Security update meetings between the CEO and Chief Security Officer take place every quarter. Security risks are also presented to the Risk and Audit Committee on a quarterly basis. This enables business leaders to become more aware of the risks, allowing the company to be better prepared.

- **OFFERING SPECIFIC GUIDANCE FOR EMPLOYEES:**

One example is to make guidelines on generative AI use (like ChatGPT) available to all employees, advising them on confidentiality, need for fact-checks, bias awareness and risk management when using such technologies.





# Conclusion

From the impact of digital transformation to the new world of work, the evolving political situation and the emergence of new technologies, the world is undergoing significant changes – changes that contribute to increased cyberthreats for states, organisations and people.

What’s more, while the nature of cyber-attacks won’t change significantly – they will still involve a perpetrator trying to obtain information and exploiting it – how they go about it will be very different thanks to technologies like AI.

As Bjørn R. Watne, Chief Security Officer at Telenor Group, points out: “Targeting humans, rather than targeting systems, is the most common type of attack. There is a saying: hackers don’t break in, they log in.”

All of this means that protection requires a combination of technological development, collaborative ecosystems and people empowerment – a multifaceted approach that Telenor embraces in its role as a telecommunications company that advances the digital world while making it safer for all.

We believe in security by design – and while technology is an invaluable part of the

solution, we also rely on the expertise of our people, for example to detect threats that fully automated systems might overlook, or to put risks into a real-world context to enable decision-making.

We also believe in the power of cooperation – both among companies, with authorities and governments, and within a wider ecosystem comprising stakeholders from research, industry, start-ups and public bodies. Cooperation is about being able to lean on each other in times of crisis and conflict – and strength comes from building security together.

Furthermore, we believe that telecommunications companies have a responsibility to support people in making sure they know how to stay safe online. We help create awareness for individuals, be they customers or employees, and we help them take control of their digital future – turning a fear of the technological unknown into accessibility, safety and peace of mind.

At Telenor, we are committed to safe and robust networks and we live up to our role of being there when society needs us – in everyday situations and in crises. We go beyond technology to empower societies.