CIO ANALYTICS

15%
have experienced major cyber attacks in the last 12 months.

Only
27%
have practiced their plan to deal with unforseen events.

NORTHERN EUROPE

2025

9 out of 10
take responsibility for sustainability.

IN-DEPTH INTERVIEWS

10
Tech with a human heart —guiding care to help people live fully, even when it's hard.

28
Building digital strength—how tech and rules help safeguard a trusted financial network.

34
Smarter seas—how AI and real-time data are redefining navigation for the maritime world.

Do you have any questions about the report? Get in touch at contact@cioanalytics.com

Contents

Page #

!

About the report
CIO Analytics is an annual survey that has been conducted in Sweden since 2018. In 2024, it was extended to cover the wider Nordic and Baltic region for the first time (referred to in the report as Northern Europe). The survey is aimed at IT decision-makers, and a total of 1,273 responses have been collected (59 per cent from the private sector and 41 per cent from the public sector).

Team
• Maria Ehrin, Sweden
• Sara Vitmosse, Tech Team
• Marita Søvik Røskar, Norway
• Carl-Eric Backman, Finland
• Giedrė Vinickienė, Baltic countries
• Mie Lin Larsen, Denmark
• Johan Bentzel, Journalist
• Local teams in all countries

The report is issued by Atea ASA, the leading supplier of IT infrastructure in the Nordic and Baltic regions.

NORTHERN EUROPEAN IT DECISION-MAKERS IN 2025:

Moving forward in winds of change

It is safe to say that the expected "new normal" post-pandemic never really happened.

Technological advances, enforced by AI, are happening faster than ever and rearranging everything from business investments to ways of work. Russia's war on Ukraine is still ongoing and the Trump administration has thrown the world for a loop. Old agreements are threatened, and new world orders are born. This affects allies, nations, and organizations—and IT decision-makers play a vital role in all of it.

The largest survey of IT decision-makers in Northern Europe has resulted in the report in front of you. Nearly 1,300 respondents have shared their insights on the challenges and opportunities ahead, helping each other create a platform for decision-making, forecasts, and leadership in what can be best described as uncertain times.

Even more than before, IT decision-makers have declared the importance of a helicopter perspective on everything that is going on, in a time when news is outdated shortly after it is published, when what is true and what is fabricated have never been more difficult to tell apart, and when a plan B—and a plan C—is always required.

It is clearer than ever that the only way forward is together.
New and improved means of collaboration, internally and between organizations, will be crucial, as will learning from those at the forefront and from the inevitable failures along the way. Taking part in the journey of others and being inspired across borders will be key to both the private and public sectors.

We hope this report supports you in outlining your roadmap for the future and that it, along with the interviews in each chapter, will bring alternative perspectives and allow you to plan and execute your next steps more confidently.

Response distribution by country of a total of 1,273 IT decision-makers in Sweden, Norway, Finland, Denmark, and the Baltic countries.

IN THE MIND OF AN IT DECISION-MAKER
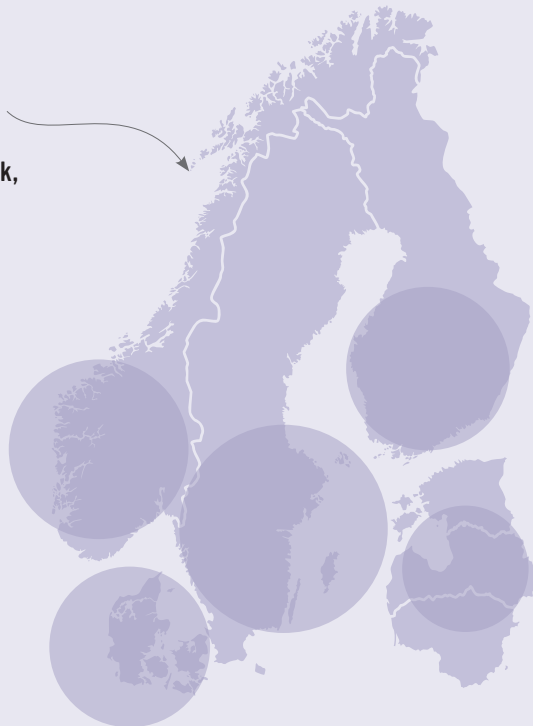
Security is an important issue in a complex world

The bar is set high for IT decision-makers in the Nordic and Baltic regions, in terms of what is expected of them and their ability to have an insight into the entire complex world that makes up the area of IT. A large proportion of the respondents in this year's report believe that a holistic perspective is the main characteristic of a good IT decision-maker.

Understanding and managing all areas of IT is hard. You must understand how digital tools can be used for educational purposes, be able to make well-founded decisions based on the needs and wishes of the business, ensure that investments in IT are cost-effective and sustainable, have knowledge of laws and risks, have good communication and collaboration skills, stay up-to-date on technical developments, and, last but not least, have the courage to test new solutions in a responsible way. This is when it becomes important to have competent employees around you.

The uncertain global situation also requires a high level of security awareness. Most of the IT decision-makers rank security as their IT organization's top priority over the next three years and many say it is the area they are likely to invest more in this year, while spending less on legacy systems.

Across all countries, the proportion of respondents who say they want to focus more on security is also increasing. It is clear that geopolitical unrest is leaving its mark and impacting on both the present and the future.

IN THE MIND OF AN IT DECISION-MAKER

A holistic IT leader is the ideal

What do you think is the main characteristic of a good IT decision-maker?

When IT decision-makers in the Nordic and Baltic countries were asked to name the main characteristic of a good IT decision-maker, having a holistic perspective came out on top. A total of 39 percent of the respondents chose this option, which is an increase of two percentage points on last year. The picture also appears to be similar in the private and public sectors (37 and 41 percent, respectively).

IT decision-makers should have a holistic perspective, but it is difficult to understand and manage all areas of IT. As an IT decision-maker, it is important to surround yourself with competent employees, advisors, and consultants.

The second most highly valued qualification overall is business understanding (27 percent), but a couple of countries stand out here. In Denmark, for example, 38 percent chose this option. One possible explanation for this is that Danish businesses—both private and public—have been at the forefront of integrating digital solutions into their core business models. This requires IT decision-makers to have a deep understanding of business strategies, and not just of technology, to ensure that IT investments are effective and lead to growth. A high level of cross-functional collaboration between IT and other business departments may increase expectations that IT

managers have a good understanding of the digital transformation and IT needs of the business, in addition to technical expertise.

Baltic IT decision-makers place strategic capabilities in second place (20 percent). Overall, however, this option only comes in third place (8 percent).

Among Finnish IT decision-makers, business understanding has gained in importance from 10 percent last year to 27 percent this year. This can perhaps be explained by the fact that business processes are playing a greater part in decision-making today. Current trends such as AI and business continuity planning are driven by business demand.

IN THE MIND OF AN IT DECISION-MAKER

More spending on security —less on legacy systems

〜〜〜〜〜〜

The IT spend will increase/decrease this year in the following areas...

Public and private sector
■ Increase   ■ Decrease

A. Security and compliance

P. Shadow IT
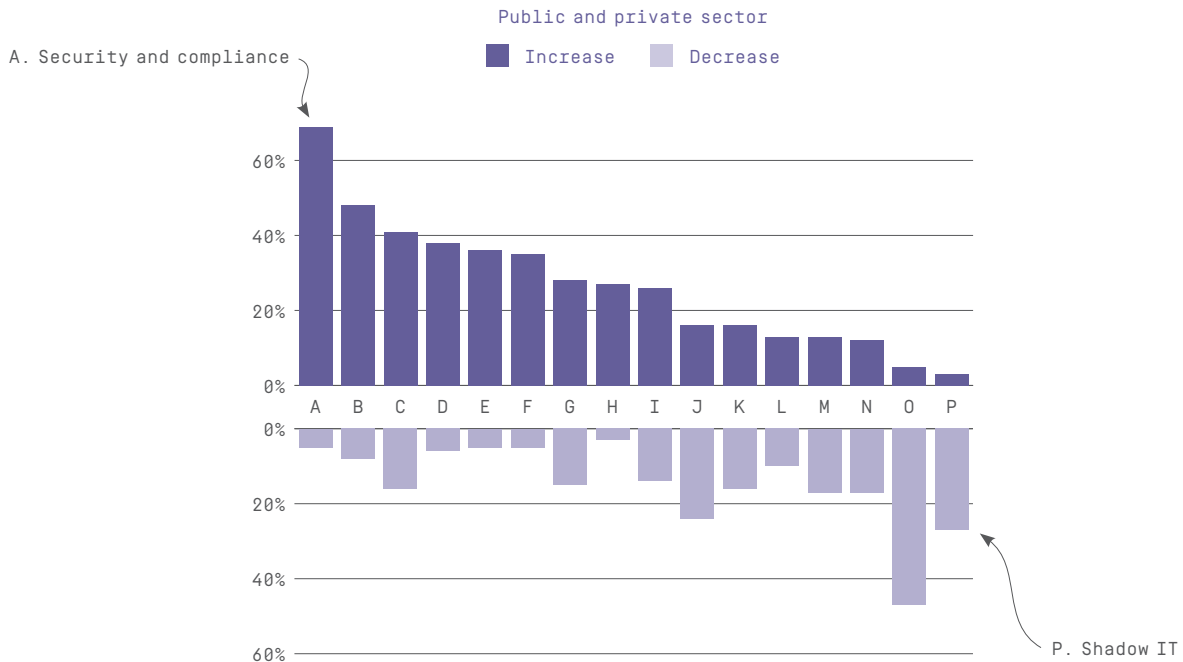
Security is the area that IT decision-makers in the Nordic and Baltic regions are most likely to spend more resources on during the year. Among respondents who list security as their primary focus (see page 8), 80 percent say that their spending on this area will increase.

This increased spending is likely due to a growing understanding of security challenges and the need for more investment. These investments are being made primarily in technology (39 percent) and people (31 percent). This prioritization is logical, as tech-nology and people form the outermost perimeter of businesses' security.

47 percent of IT decision-makers are reducing their spending on legacy systems, making it the area where spending is declining the most. Other areas where IT decision-makers are decreasing their spending are shadow IT (27 percent) and hardware (24 percent).

However, in all areas there are some decision-makers who are still increasing their costs. For example, 16 percent of IT decision-makers are raising their spending on hardware.

A. Security and compliance
B. Cloud services
C. Licenses and subscriptions [SaaS]
D. Digital transformation
E. Developing AI models
F. Data and analytics
G. New applications and systems
H. Existing AI services
I. Projects and development
J. Hardware
K. IT support and personnel
L. Workplace and collaboration
M. Telecom and networking
N. Datacenter and edge
O. Legacy systems
P. Shadow IT

Multiple-choice question

IN THE MIND OF AN IT DECISION-MAKER

Security remains the top priority

What are your IT organization's top priorities over the next three years?

Public sector
2025   2024

Private sector
2025   2024

Multiple-choice question
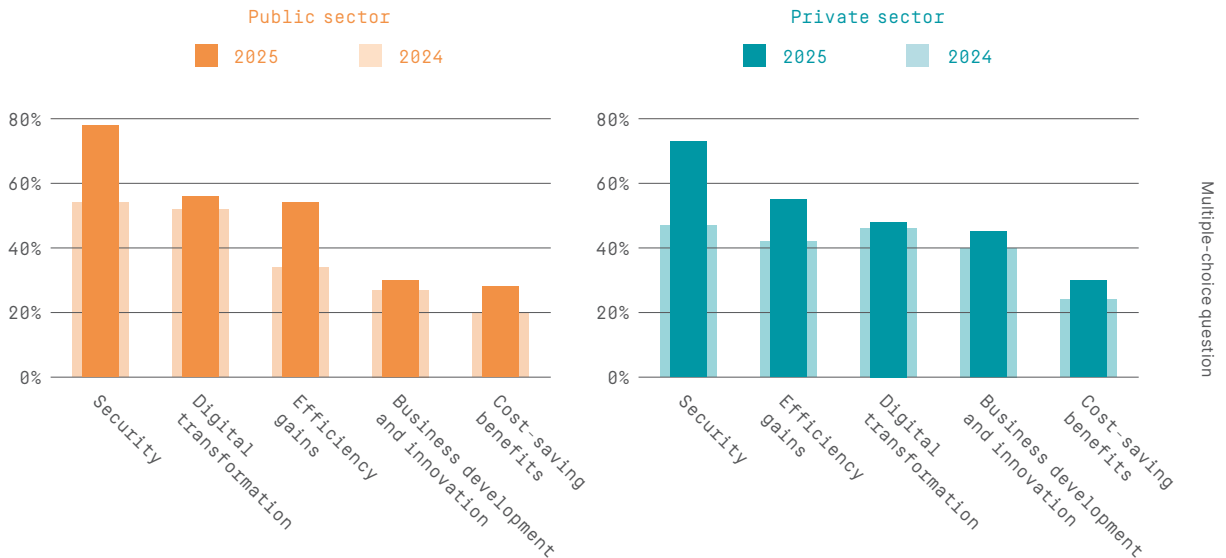
In the current global situation, it is not surprising that security is the top priority among IT decision-makers in the Nordic and Baltic countries for the next three years. This has made gains since last year, rising from 50 to 75 percent. However, it is important to bear in mind that information security, which was a separate answer option last year, is now incorporated into security in general. The increased interest in security is also clearly shown in other parts of this report.

Security always has to be considered as part of new digital initiatives and in all digital transformations. New technologies, such as AI, must balance innovation with security. According to the international audit and advisory firm KPMG ("Investing in cybersecurity to safeguard innovation"), this often leads to a reallocation of resources to ensure that new digital initiatives are secure from the outset.

Other priorities that have become more prominent are efficiency (from 38 to 55 percent) and digital transformation (from 48 to 51 percent). In Finland, digital transformation is also a high priority, especially in the public sector (51 percent). NATO membership and the need for structural reforms in social welfare are strong drivers in this respect.

Overall, in the Nordic and Baltic countries, 39 percent of the respondents state that business development and innovation will be a priority area over the next three years, but the corresponding figure in Norway is only 20 percent.

Norwegian IT departments also generally rank themselves lower on the proactivity scale. In the Baltic countries, 55 percent indicate business development and innovation as a top priority. There are several explanations for this: For one thing, the limited domestic market requires a greater focus on foreign markets. The EU contributes substantial funding for digital transformation, which many want to tap into. There is a high level of awareness of the importance of keeping up with technological developments and ensuring that employees adapt to new tools and digital processes. In addition, AI and other digital tools can be used to help resolve the shortages in staff that many companies may face in the future.

IN THE MIND OF AN IT DECISION-MAKER

Security is the primary focus—but digital transformation is on the rise

What is currently your primary focus in your role as an IT decision-maker?
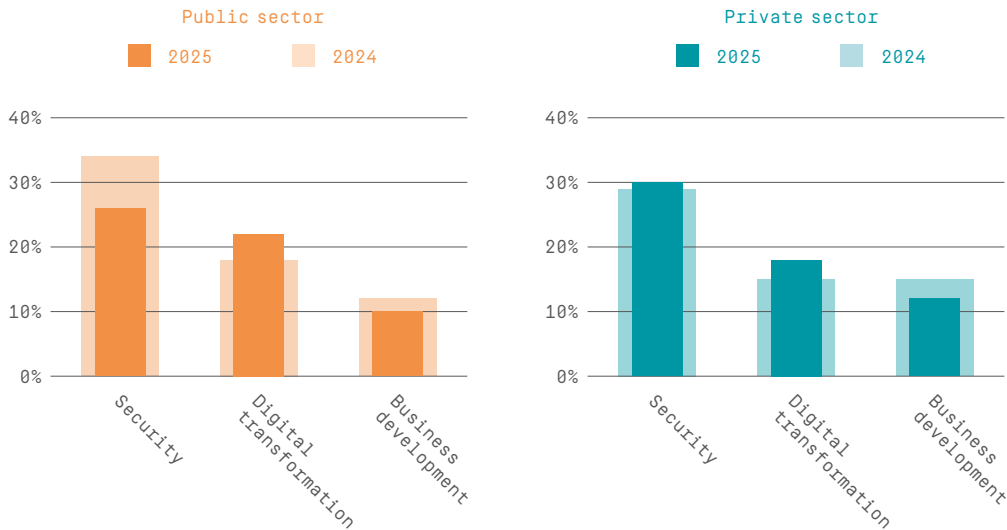
Security runs like a common thread throughout this report, including on the topic of primary focus. 30 percent of respondents in the private sector and 26 percent in the public sector cite security as their primary focus. There is also a clear connection between giving this response and ranking security significantly higher as the "biggest challenge last year" and the "biggest challenge next year" (see pages 18–19). As companies heighten their focus on security, it also becomes clearer what measures are needed to reach the level of security they want to achieve.

In general, in the private sector, the focus on security remains high.

However, IT decision-makers from large companies tend to focus less on security and more on digital transformation. They are also often further along in their AI development and see themselves more as practitioners (36 percent, compared to an overall average of 20 percent). They are ready to change focus. AI and other projects within digital transformation, which are seen as crucial for competitiveness and growth, require large investments. As a result, resources often have to be reallocated from other areas. Organizations are prioritizing initiatives that can improve operational efficiency, enhance customer experiences, and open new revenue

streams (read more on page 33 about how AI has contributed to value). Security is still an important issue, but many large organizations have probably already made major investments in cybersecurity in recent years and feel that they can maintain security with less investment.

In the public sector, security is declining as a primary focus, having fallen from 34 to 26 percent, although it is still ranked at the top. At the same time, digital transformation, cost savings, and skills supply are gaining. One possible explanation for this is that in 2025 the public sector will be more affected by cuts and reduced budgets than by new security investments.

IN THE MIND OF AN IT DECISION-MAKER

A desire for more of a focus on business development and digital transformation

What would you like to focus more on in your role as an IT decision-maker?
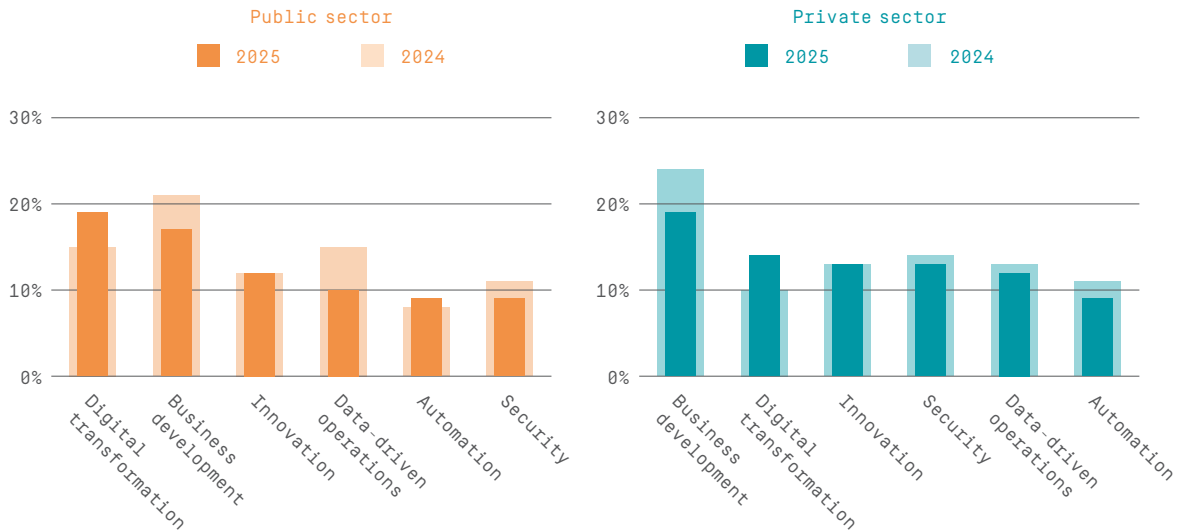
As seen in other parts of this report, security remains an important focus area for IT decision-makers in the Nordic and Baltic regions, but there are significant differences between countries. While just under 10 percent of IT decision-makers in Sweden, Denmark, and Finland state that they want to focus more on security (7, 8, and 10 percent, respectively), 18 percent want to do so in Norway. This may indicate that a security-oriented mindset plays a larger part in the role of Norwegian IT decision-makers.

In Sweden, Denmark, and Finland, the inclination is more toward a greater focus on business development and digital transformation. As was the case last year, these two areas are also what IT decision-makers in the Nordic and Baltic countries want to focus more on in general.

Last year, 23 percent of the respondents stated that they focus most on business development. This year, this figure dropped to 18 percent. At the same time, digital transformation increased from 12 to 16 percent. The reduced gap may be due to more IT decision-makers seeing the connection between digital transformation and the realization of their business goals.

Within the private sector, 19 percent of the respondents want to focus more on business development and 14 percent on digital transformation. In the public sector, it is the other way round, with 19 percent preferring to focus on digital transformation and 17 percent on business development.

Above all, it is municipal IT managers who want to focus more on digital transformation (21 percent), possibly because other businesses have already invested a lot in this area, while municipal organizations have fallen behind.

A human compass in a digital reality

Thomas Buchwaldt leads the digital development at OK-Fonden – a non-profit care organization with 2,500 employees and services spanning nursing homes, psychiatric residences, and hospices. But when he talks about technology, it's not just about bits and bytes. It's about people. About living life, your whole life, even when it's hard.

Thomas Buchwaldt, CIO, OK-Fonden.

In a reality shaped by artificial intelligence, geopolitical unrest, and rising expectations for service and efficiency, it can be tempting to put technology in the driver's seat. But Thomas Buchwaldt, CIO at OK-Fonden, insists on starting somewhere else: With the culture, the strategy, and the people who are using the solutions. For him, digitalization is not a destination, it's a tool for creating cohesion and dignity.

"We don't talk enough about what we actually want to achieve with technology," he says. "It's not just about functions and operations; it's about supporting the organization's goals and making sure our people thrive."

This holistic approach defines OK-Fonden's entire digital strategy. Here, IT isn't just a tool, it's an integrated part of the core mission. And speed is not a goal in itself. "We don't aim to be first movers—we aim to be smart movers. It's about being able to act quickly, with peace of mind."

According to Thomas Buchwaldt, expectations have risen among employees, residents, and relatives alike. Technology must be intuitive, efficient, and meaningful. "People are used to seamless solutions in their private lives, and they expect the same in their professional environment. We must match that sentiment and translate it into our context."

That's why balancing innovation with stable operations begins with understanding end users. "We know it's not us at headquarters who use the systems, it's the staff at the nursing homes and residential units. That's why we need to go out and listen carefully to their daily reality."

One such example is a pilot project using smartphones and Samsung DeX, which simplifies medication documentation directly at the resident's side. "We call it balanced innovation. We're not chasing buzzwords; we're focusing on what creates real value."

Cyber and information security are more important than ever. For Thomas Buchwaldt, NIS2 isn't just a directive, it's common sense. "We manage sensitive personal data, and we must meet the highest standards, whether we are officially subject to the directive or not. Cybersecurity is our license to operate."

To make room for strategic priorities and focus on the core business, OK-Fonden has outsourced its entire IT operations. That frees up resources for development instead of maintenance. At the same time, IT's role in top management has been strengthened through recurring meetings that focus on goals, not technology. "We don't talk much about the screwdriver, we talk about the house we want to build," he says.

"In a complex reality, it's not necessarily the fastest code that gets you ahead. It's the ability to think holistically, act strategically, and remember why you started."

2

RESPONSIBILITIES OF AN IT DECISION-MAKER

Proactive organizations create new business opportunities

More and more IT departments believe they are proactive in relation to meeting business needs or claim to be moving in that direction, while the proportion of reactive IT departments is falling—which is good news. Proactive organizations may not stand out in terms of results, but they have fewer skills-related needs and more technology in production, while reactive IT departments focus more on maintaining existing systems. In addition, proactive organizations are investing more in artificial intelligence (AI) solutions that can help the business move forward and create new commercial opportunities.

Yet fewer than half of all IT departments state that they are evaluated based on how they contribute to the organization's goals. Budget and finances are still the most common basis for measuring their performance. IT transformation is a considerable part of an organization's digital development. It is important to assess these projects based on cost, time for implementation, and delivered functionality—but most importantly, to evaluate how they create business value too. The collaboration between business and IT is strengthened if IT transformation is linked to business gains. This also means that initiatives that benefit the business and the organization as a whole will be given higher priority.

Overall, IT decision-makers are taking responsibility for fewer areas of sustainability in relation to the company's sustainability goals compared to last year. At the same time, the demand for sustainability experts has doubled. New regulations and requirements are driving development and creating a greater need to collect and report sustainability data. This generates opportunities for IT departments not only to report this data, but also to take greater responsibility for the organization's core IT components relating to sustainable data centers, operations, life cycle management, and so on. This may mean that sustainability will become a core IT competency and not just a compliance task.

Budget remains the most common basis for evaluation

How is the IT organization measured and evaluated?

Public sector
■ 2025 ■ 2024

Private sector
■ 2025 ■ 2024
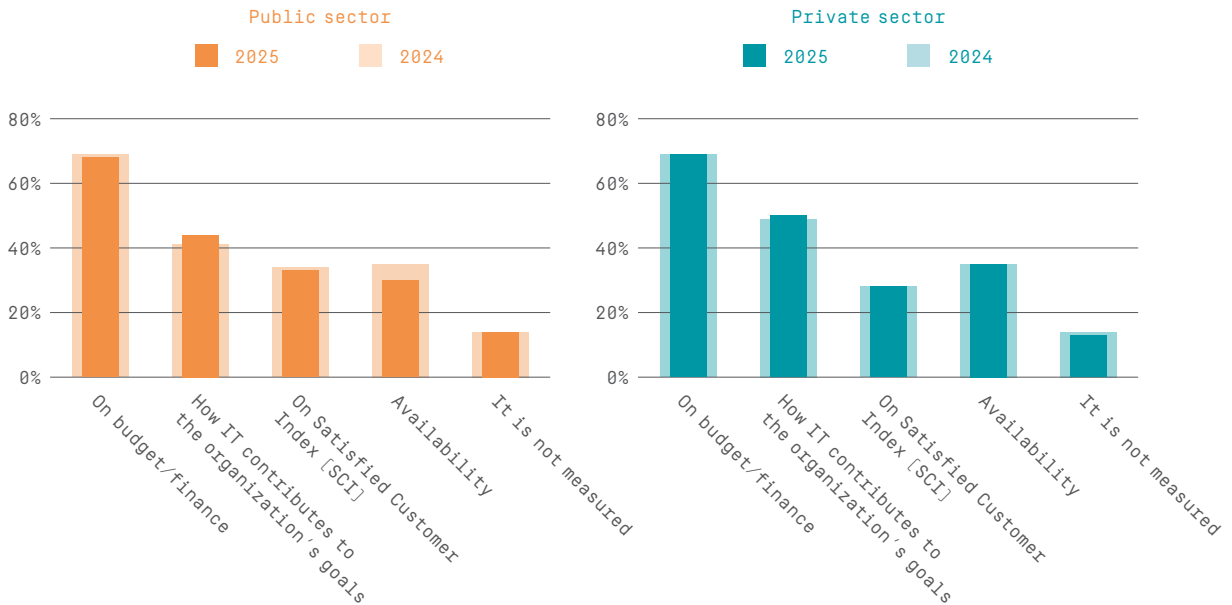
Regardless of country or sector, most IT organizations are, unfortunately, still primarily evaluated based on budget and finance. Only 48 percent are assessed based on how they contribute to achieving business goals (read more on page 14 about how the rest of the organization views IT). Measuring how IT contributes to business opportunities is significantly more difficult than evaluating the costs. Even in the Baltics, where

contribution to goals is actually the most common basis for evaluation, the percentage assessed on budget is increasing (from 44 to 50 percent).

More IT decision-makers in the private sector say they are assessed on contribution to goals than those in the public sector: 50 compared to 44 percent. Irrespective of sector, proactive organizations are more frequently evaluated based on their contribution to business

goals—60 percent in total (see page 13). Only 35 percent of those with a reactive approach are assessed in this way. Value-creating measures might be more beneficial to the business and also steer the organization toward a more proactive mindset. A matrix weighing value against effort could help link business development and digital transformation to activities that create high value with limited effort (see page 14).

Proactive organizations invest more in AI

Do you consider your IT organization to be proactive in terms of what your business needs?

Public sector
■ 2025   ■ 2024

Private sector
■ 2025   ■ 2024

1. Yes, we proactively meet the needs of the business.
2. No, but we are moving towards a more proactive way of working.
3. No, we act more reactively when it comes to what the business needs.
4. Other.
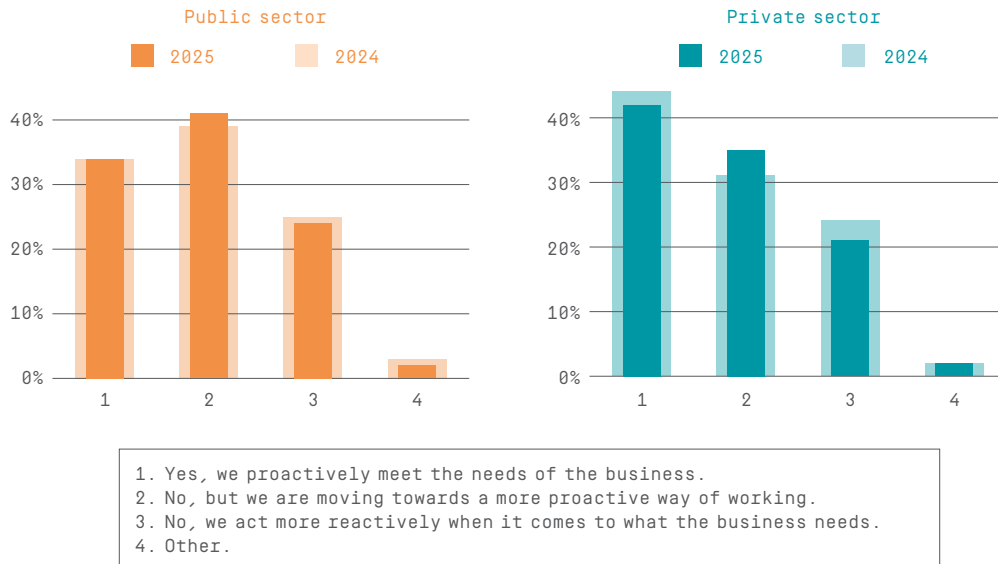
The percentage of IT decision-makers who say they take proactive action aimed at meeting the needs of their business is stable, or perhaps even showing a tendency to decline. On the other hand, the proportion of organizations moving toward a proactive approach has increased (from 34 to 37 percent), while those acting reactively have decreased from 24 to 22 percent. Overall, this still indicates a development in the right direction.

Although some organizations see themselves as proactive, it is hard to find a direct link to improved results. However, their need for skills and expertise is less significant (see page 21) and they also have more technologies in their production operations,

such as AI (see page 30). In addition, these proactive IT departments are rarely seen as a necessary cost by their respective organizations, while reactive ones are more often viewed in this way (see page 14).

There is also a connection between acting reactively and investing less in both new and existing AI services, data and analysis, and projects and development (see page 6). This suggests a certain degree of caution and a willingness to prioritize existing systems rather than developing new solutions.

Proactive organizations generally have greater AI maturity and also seem more willing to invest in the development of both new and existing AI models. The same applies to

attitudes toward and use of cloud services. 76 percent of all proactive organizations have a positive attitude toward public clouds, compared to 65 percent among reactive organizations.

Organizations moving toward a proactive approach are reducing their shadow IT spending at an above-average rate (see page 6): 33 percent compared to 27 percent. This may be because proactive organizations are optimizing their IT resources and reducing inefficiencies and potential security risks. By spending more on AI development, these organizations are better positioned to adapt to future technological advances, indicating a commitment to innovation and growth.

With IT involved in management, more people see how important it is for efficiency

The rest of the business sees the IT department as a...

Public sector   **Private sector**

Public sector pie chart: 54%, 21%, 11%, 9%, 5%

Private sector pie chart: 43%, 20%, 18%, 14%, 4%

Legend:
- Critical element for efficiency and digitalization
- Necessary cost
- Business partner
- Business enabler
- Other
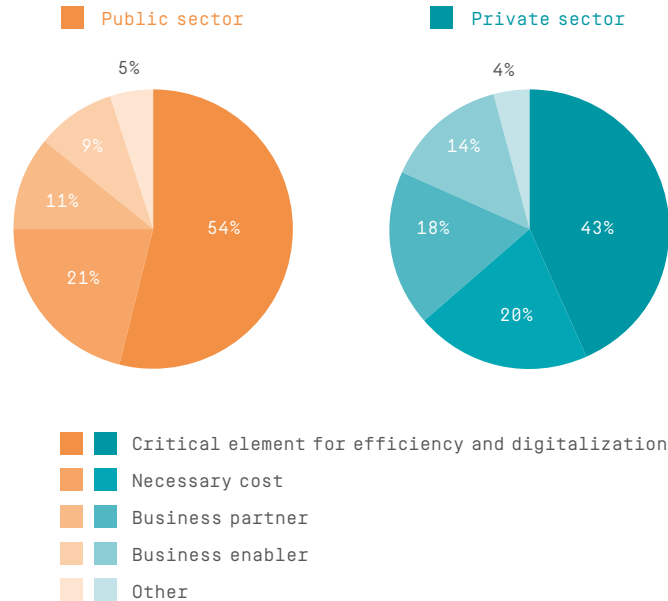
Among IT decision-makers who are part of the top management of their organization, 51 percent responded that IT is considered important for efficiency and digitalization, while 45 percent of those at lower organizational levels said the same. 25 percent of these lower-ranked IT decision-makers state that the IT department is seen as a necessary cost, while the corresponding figure among those at top managerial level is 14 percent.

The IT department can be viewed in many ways, but there are generally two predominant viewpoints: They are regarded either as a function for operations and maintenance or as an active participant in business development through the utilization of new technology and digital opportunities. Above all, it is the position and status of the IT department within the organization that affects this attitude, as well as the prevailing views on business development and digital transformation. In the one case, digital transformation is primarily seen as a way to develop IT operations, while in the other it has a very significant part to play in the company's development and business opportunities in general.

In many cases, the role of the IT department, and therefore how it is viewed, depends on the size of the organization. Small organizations often have less opportunities for specialization and a more limited ability to contribute to business goals than large ones. At the same time, medium-sized organizations can struggle to find the right level of specialization and division of responsibility, which can lead to inefficiency as they often switch between different solutions.

By taking on more responsibility for data and information, there is great potential to be proactive and to be an active participant in business development. Businesses with a high level of maturity in data-driven development often use information to make quick decisions and adapt to new needs and risks. A matrix weighing value against effort could be a way to measure the effectiveness of the IT function, by linking business development and digital transformation to activities that create high value with limited effort. Read more about how IT is evaluated on page 12.

The need for sustainability expertise has doubled

What do you consider to be your responsibility as an IT decision-maker when it comes to the company's sustainability goals?

Public sector — 2025, 2024
Private sector — 2025, 2024

Multiple-choice question
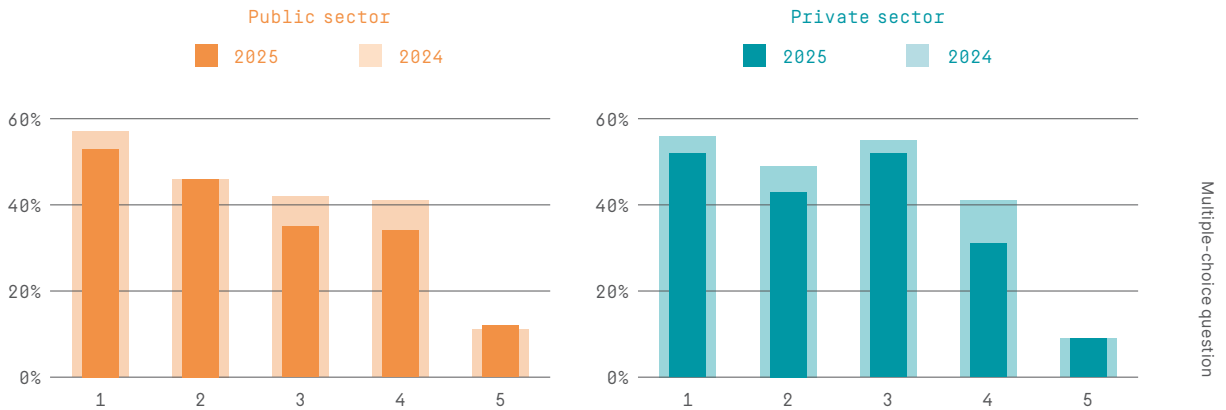
1. Set and follow up sustainability goals for IT operations.
2. Digitalize business processes to achieve the company's sustainability goals.
3. Support and streamline the internal sustainability work of the business using IT and analytics tools for data collection and visualisation.
4. Support the development of products and services that help customers achieve their sustainability goals.
5. None of the above is part of my responsibility.

The development of new technologies and digital transformation are becoming increasingly important for sustainability work. Organizations whose IT departments consider themselves responsible for setting sustainability goals are also more likely to align their IT strategy with these goals. Organizations that do not align their digital strategies with sustainability goals often have IT decision-makers who do not see sustainability as their responsibility.

In this year's report, 10 percent of all IT decision-makers responded that they have no responsibility for their organization's sustainability goals. 32 percent of these also do not consider environmental or social sustainability in their strategies, compared to an average of 12 percent for all respondents. In addition, they generally act more reactively to business needs (see page 13).

It is clear that a lack of responsibility for sustainability generally weakens IT strategies, sometimes to the point of not having a formal strategy in place at all. Most IT decision-makers who do not take responsibility for sustainability goals are based in smaller IT departments, while larger IT departments have to a greater extent aligned their IT strategies with sustainability goals. IT managers who are part of the top management are also more likely to invest in sustainability.

The need for sustainability expertise in the Nordic and Baltic countries has doubled, albeit from a low level: from 5 to 10 percent. The increase is greatest in Finland, where the figure has jumped from 5 to 16 percent (see page 21). This indicates that sustainability is on its way to becoming a core competence in IT, and not just a compliance task. Extensive EU regulations and demand for sustainability data also require significant resources.

However, there is a decline in several of the sustainability areas that IT decision-makers consider themselves responsible for, such as setting and following up on goals, supporting and streamlining internal sustainability work, digitalizing business processes to achieve the company's sustainability goals, and contributing to the development of products and services that help customers achieve their own sustainability goals. Overall, IT decision-makers are taking responsibility for fewer areas of sustainability in relation to the company's sustainability goals compared to last year.

RESPONSIBILITIES OF AN IT DECISION-MAKER

Ponsse processes trees and data according to their intended use

Ponsse, a Finnish listed company, is one of the world's leading manufacturers of forestry equipment. The company also develops digital solutions that support the planning, management, and monitoring of timber harvesting and enable the efficient use of data from forest machines.

Miika Soininen, Director of IT and Digital Services, Ponsse.

"**Forest machines** are still at the core of our operations, but we have built a comprehensive service business and a growing suite of digital services around them. We are developing all of these in parallel, and also fitting them together," says Miika Soininen, Director of IT and Digital Services at Ponsse.

Founded in 1970, Ponsse has grown into an international group with more than 2,000 employees, while still remaining a family-owned business. The company makes use of advanced technology and develops digital services in close cooperation with its customers. Interface services were the first to be commercialized, ensuring the direct transfer of information to customers' systems through interfaces.

"Paying attention to customer needs and listening to feedback is typical for us. We do not innovate simply because some new technology is available. We always develop services to meet our customers' actual needs," Miika Soininen says.

Ponsse has already delivered more than 21,000 forest machines to its customers. The company specializes in cut-to-length machinery that allows both felling and processing the trees in the forest according to their intended use.

At the same time, the machines collect a tremendous amount of data on the felled and cut trees, fuel consumption, and the harvesting location, for example. They also optimize the route travelled in the forest. Only some of this data ends up with the customer as it is. Miika Soininen emphasizes that data is only valuable when it has a clear purpose.

"**Nowadays, forestry** machines produce a huge amount of data, but it is not worth collecting it just for the sake of collecting it. You must identify what is essential and use it wisely. We ensure that data is transferred from the forest machines to the customer in a ready-to-use format. This way, the customer can build their own reporting, ERP, or application directly on top of the data that they receive from us. Our service department also benefits from data and can continue to serve our customers better."

At Ponsse, IT and software development are both closely integrated into the business.

"We have integrated our software and product development more closely with a traditional IT department and are consciously seeking synergies between them. As an IT organization, we aim to be a flexible partner that finds solutions together with the businesses," Miika Soininen says.

The services developed for customers and internal IT development needs are separate entities, and their needs are considered separately. Decisions on their prioritization are made in collaboration with the business areas. Transparency and good communication are key parts of that process.

Ponsse's development work is built on a combination of customer understanding, technological expertise, and bold development. IT is a strategic and important part of the company's business.

"We encourage experimentation and give responsibility to do and learn. We also accept that not all experiments lead to anything. We are open-minded in exploring the possibilities of new technologies, such as artificial intelligence," says Miika Soininen.

3

Security challenges increase demand for skills and expertise

Security is both next year's biggest challenge and what IT decision-makers in the Nordic and Baltic regions are prioritizing the most going forward, although there are some differences between countries.

In particular, Sweden and Denmark highlight security as a primary challenge, while Norway and Finland are slightly more concerned about resources. The overall proportion of respondents who see security as their biggest challenge next year has decreased to some extent, although this area still ranks as the most important. This may be because security is no longer seen as a standalone issue to be resolved once and for all, but as a natural element of ongoing work.

The importance of security is apparent in the skills and expertise that are in demand in the IT industry. Over half of the respondents in this year's report are in need of security experts, which is a clear indication of a skills shortage in this area. Expertise is brought in through suppliers, rather than through hiring, which is expensive in the long run.

The demand for change management is clearly increasing. This is likely due to an increased focus on digital transformation, where artificial intelligence (AI) and other systems can also potentially contribute to enhancing security. IT architects and cloud experts are also in high demand. In an ideal scenario, this could open up new opportunities for bringing more women into the IT industry, as the proportion of female IT specialists is still very low and has not changed significantly since last year. However, in several of the countries surveyed, the proportion of women studying for technical professions is increasing, which bodes well for the future.

Major differences in views on security challenges

What was your IT organization's biggest challenge last year?
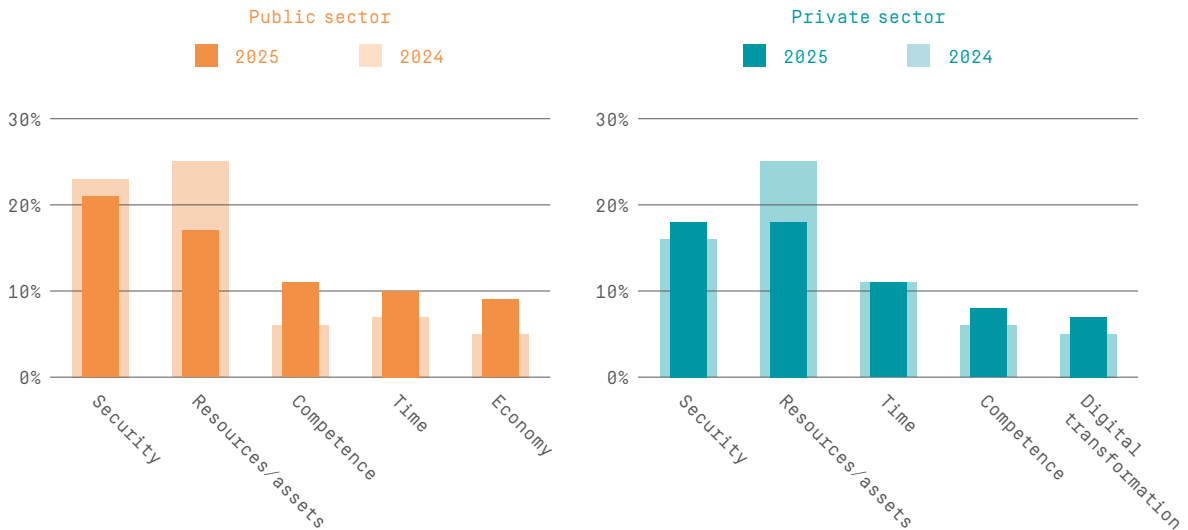
In last year's report, resource availability was highlighted as "the biggest challenge last year." This year, this figure has fallen from 25 to 18 percent. This development is reinforced by the fact that expectations for next year also point to resource availability as less of a challenge than previously (see page 19). This apparent improvement in resource availability may be due to the recession and the fact that there is more labor available, while companies are currently not hiring as much. With more applicants per position, it is also easier to find the right resources.

In both Sweden and Denmark, security is ranked as the top challenge last year, at 28 and 21 percent respectively, compared with an overall average of 19 percent. In Norway,

which like Finland ranks resources as last year's biggest challenge, the corresponding figure is only 12 percent.

Why does Sweden rank security so high as a challenge and Norway rank it so low?

In Sweden, NATO membership has attracted a lot of attention to the country. Many organizations have been subjected to major cyberattacks, while gang wars also have caused turmoil. This has raised the bar for what must be considered "the new normal" in terms of the challenges that organizations have to face and defend themselves against.

Security is a key focus and top priority for the next three years, but the primary challenge cited by IT decision-makers in Norway is

resources/assets. One Norwegian respondent explained that the biggest challenge next year is to catch up in terms of both technology and processes, which is important for the continued digital transformation process. Although there are clear goals, the path is not as clearly defined, mainly due to a lack of resources and competence. To meet this challenge, the IT department must strengthen the team's skills, prioritize tasks better, and work more strategically to link IT investments to the company's long-term vision. At the same time, better resource management and collaboration across departments must be ensured to create a more integrated and effective approach to digital transformation.

Security continues to be the biggest challenge

What do you think will be your IT organization's biggest challenge next year?

Public sector
■ 2025   ■ 2024

Private sector
■ 2025   ■ 2024
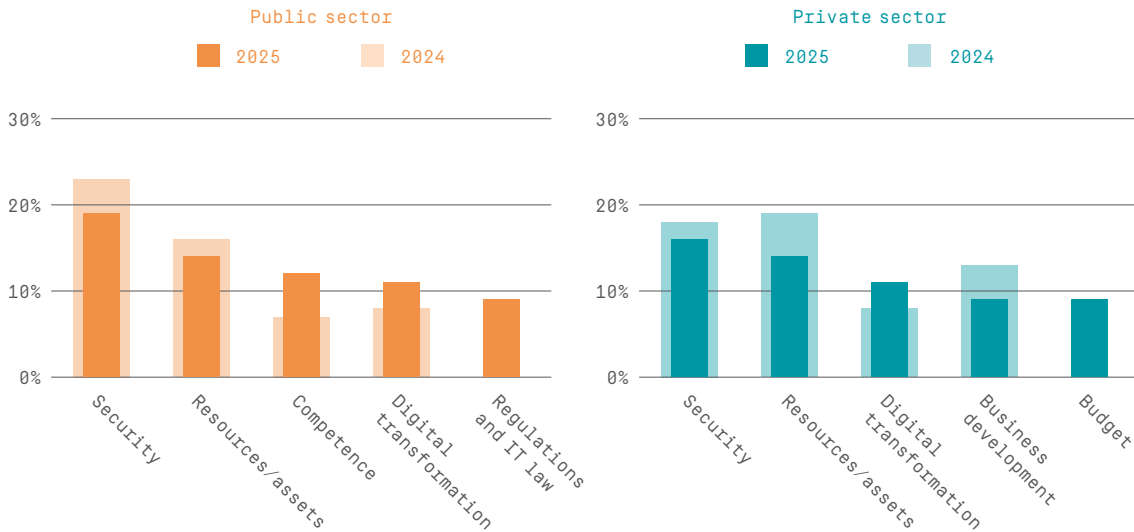
It should come as no surprise that security comes out on top when IT decision-makers in the Nordic and Baltic regions identify next year's biggest challenge. Security is also highlighted as next year's top priority (see page 7) and this is reflected in the skills and expertise in demand too (see page 21). This suggests that many organizations have a skills shortage when it comes to security, which emphasizes the need for outsourcing services in this area and the requirement for close partnerships with security experts. The focus on implementing the EU's NIS2 Directive on cybersecurity is mentioned in several of the responses, regardless of country.

In the 2024 report, 27 percent of Swedish IT decision-makers stated that security would be their biggest challenge next year. The corresponding figure this year is 18 percent. Security is still at the top, but the decrease may be due to this area not being seen as the standalone challenge to be solved once and for all, but as a natural part of ongoing work. This shows an increase in maturity. At the same time, the political and economic instability in the world means that other, equally important issues have to be addressed too. This can affect how IT departments prioritize their tasks and challenges.

More respondents in Denmark than in other countries highlighted regulations and IT law as the biggest challenge next year—it is the second biggest challenge in Denmark overall.

The country is well ahead in this area and is known for its high standards when it comes to data protection and privacy laws. In particular, this is a major focus in the financial and public sectors, and also within the huge pharmaceutical industry.

The second biggest challenge overall next year is resources/assets. In last year's report, 28 percent of IT decision-makers in Finland ranked this area as the biggest challenge for next year. This figure has now dropped to 13 percent. Instead, budget is ranked as the biggest challenge in Finland. Getting hold of resources is now not only a matter of finding the right resources to employ, but more about having—or getting—the money to employ them.

Women still underrepresented in IT

How many women work in your IT department?

■ Public sector ■ Private sector

24.3% [25.8% in 2024]

17.7% [18.1% in 2024]
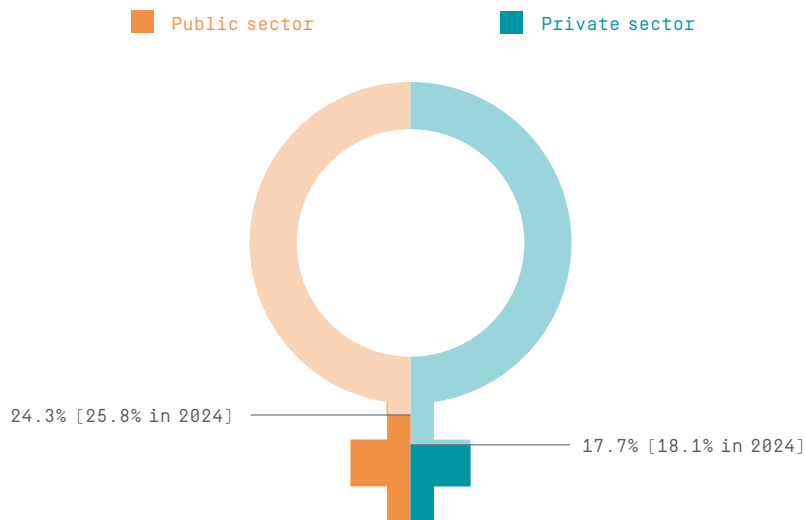
Only a fifth of the employees in IT departments in the Nordic and Baltic countries are women. Even though many women are drawn to the technology industry, the proportion of female staff in IT departments does not seem to be increasing.

Just like last year, Norway stands out with the lowest proportion of women in both the public and private sectors: 18 and 14 percent, respectively. In Norway, there are still disparities leading to an unequal distribution of economic resources between genders in the workforce. Women and men hold different occupations and are employed in different industries. More women work in the public sector, while the private sector is male-dominated. 29 percent of the employees in the technology industry in Norway are women, but the average in IT departments is 15 percent. 42 percent of all organizations have no women at all in their IT departments—a figure that rises to 50 percent in the private sector.
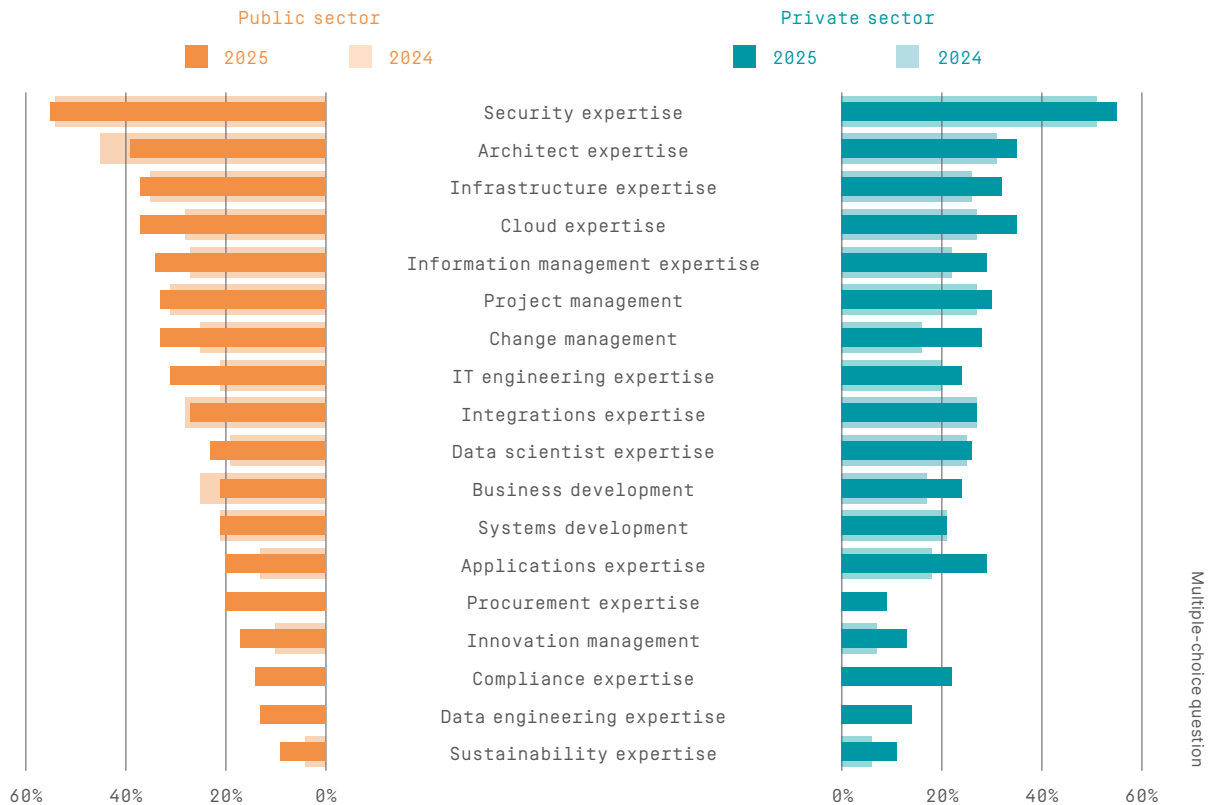
In all the countries featured in this report, the proportion of women in IT departments is low, especially in the private sector. The reason for this is probably that fewer women choose to study STEM subjects (science, technology, engineering, and mathematics). In the Baltics, this may be due to a lack of knowledge among young people about the diversity of opportunities available in the IT sector, which is often presented in a very narrow way at school. This creates a misleading impression that IT is only about programming. Overall, in the Nordic and Baltic countries there are also fewer female role models in the industry and, in some cases, an exclusionary work culture.

IT is a broad professional area with many roles to fill. The range of skills and expertise needed is large and diverse (see page 21). The individual tasks involved need to be highlighted more, rather than maintaining an outdated and false image of IT. Shining the spotlight on this is important in all countries and could probably attract more women to the industry. There are already signs of change in many countries: The proportion of women who opt for IT subjects as their first choice has increased, for example. There are also indications, in Denmark for instance, of a positive trend regarding equal pay for women and men in the IT industry. In Sweden, however, current salary statistics from the Swedish trade union Naturvetarna show that the present gender pay gap in the IT industry is the largest since 2014.

High demand for security experts

What competences will your IT organization need within the next 12 months?

Public sector — 2025 / 2024
Private sector — 2025 / 2024

Security expertise
Architect expertise
Infrastructure expertise
Cloud expertise
Information management expertise
Project management
Change management
IT engineering expertise
Integrations expertise
Data scientist expertise
Business development
Systems development
Applications expertise
Procurement expertise
Innovation management
Compliance expertise
Data engineering expertise
Sustainability expertise

Multiple-choice question

There is an increase in the demand for skills and expertise in almost all areas. Demand is particularly high for security experts (55 percent), IT architects (37 percent), and cloud experts (36 percent). The geopolitical climate continues to be uncertain, with an increased number of cyberattacks as a result, and this has an impact on the type of skills in demand. Higher demand may provide an opening for bringing more women into the industry (see page 20).

The most noticeable difference between last year and this year is in the demand for change management, which has increased from 20 to 30 percent. Demand is increasing throughout the Nordic and Baltic regions, regardless of the sector or size of the organization. There seems to be a connection between the need for change management and an increased focus on digital transformation (see pages 7–9).

The demand for security experts is slightly higher in Finland than in the Nordic and Baltic countries as a whole (60 percent compared to 55 percent). The service structure reform of social welfare has given rise to skills gaps and difficulties in finding the right expertise. Instead of having their own employees, organizations

must buy these skills from service providers, which entails high costs.

In Denmark, the demand for compliance experts stands out in particular, at 32 percent compared to 19 percent for the report as a whole. This is also in line with the challenges Denmark is seeing with regard to regulations and IT law. One possible explanation before this is that upcoming legislation in the financial and public sectors has already been implemented in some public framework agreements. Denmark is also home to many pharmaceutical organizations, with higher regulatory standards to adhere to.

Navigating IT challenges in public broadcasting: The LRT success story

Last year, LRT (Lithuanian National Radio and Television) held its annual "Golden Bee" awards to recognize outstanding employees. To his surprise, Donatas Jovarauskas, the Head of IT, found himself not only nominated but also winning this prestigious internal recognition. The award reflects the significant transformation LRT's IT division has undergone under his leadership.

Donatas Jovarauskas, Head of IT, LRT.

As Lithuania's national broadcaster, LRT spans three media platforms: radio, television, and an online portal. By law, its radio and television operations are classified as critical infrastructure. Despite limited resources, the IT division must maintain absolute reliability while still embracing innovation.

To address these challenges, Donatas Jovarauskas merged all IT functions, previously spread across teams, into one division. This strategy follows best practices from the European Broadcasting Union, of which LRT is a member. An Operational and Project Management division was also established to streamline workflows, manage contracts, and keep projects on track.

Balancing the needs of critical infrastructure with limited budgets requires strategic planning. At LRT, the budget aligns closely with long-term goals: The board sets directions, leaders define priorities, and divisions adjust accordingly. "Our three-year budget cycle reflects these shared goals and helps us stay focused," Donatas Jovarauskas explains.

A key element of this approach is what he calls "mathematical IT management." Instead of adding staff, the focus is on understanding root causes and setting priorities —resulting in smarter resource use.

Part of this optimization effort also aligns with the organization's commitment to sustainability. "We rent or purchase technology as a service, reducing waste and avoiding unnecessary resource use. Even issuing new computers can waste time—they might sit in storage for 2-3 months before being distributed," he notes.

Efficiency also guides LRT's cybersecurity strategy. Instead of building a costly 24/7 internal monitoring team, they outsourced security operations center services. This allows for automated threat detection without needing a large in-house team.

Donatas Jovarauskas emphasizes a crucial insight about cybersecurity that shapes the division's educational efforts: "Hackers don't break into systems—they log in with stolen credentials." This understanding drives his focus on employee awareness rather than solely technical solutions.

Aligning with LRT's organizational values, Donatas Jovarauskas has built a diverse IT team that maximizes the contribution of every member. "The division includes nearly 30 people with very low turnover," he explains. Women hold key leadership roles—a significant achievement in the traditionally male-dominated IT field.

His people-centered leadership philosophy is essential to making the most of limited human resources. "It's work with people and for people—both inside the organization and in the country," Donatas Jovarauskas notes.

"What drives me? I appreciate the depth of this journey—the extensive scope of activities that need to be encompassed from that bird's-eye view," Donatas Jovarauskas reflects. His balanced perspective, combining rational resource management with genuine care for people, enables LRT to deliver essential public broadcasting services despite the ever-present challenges of limited time, assets, and resources.

4
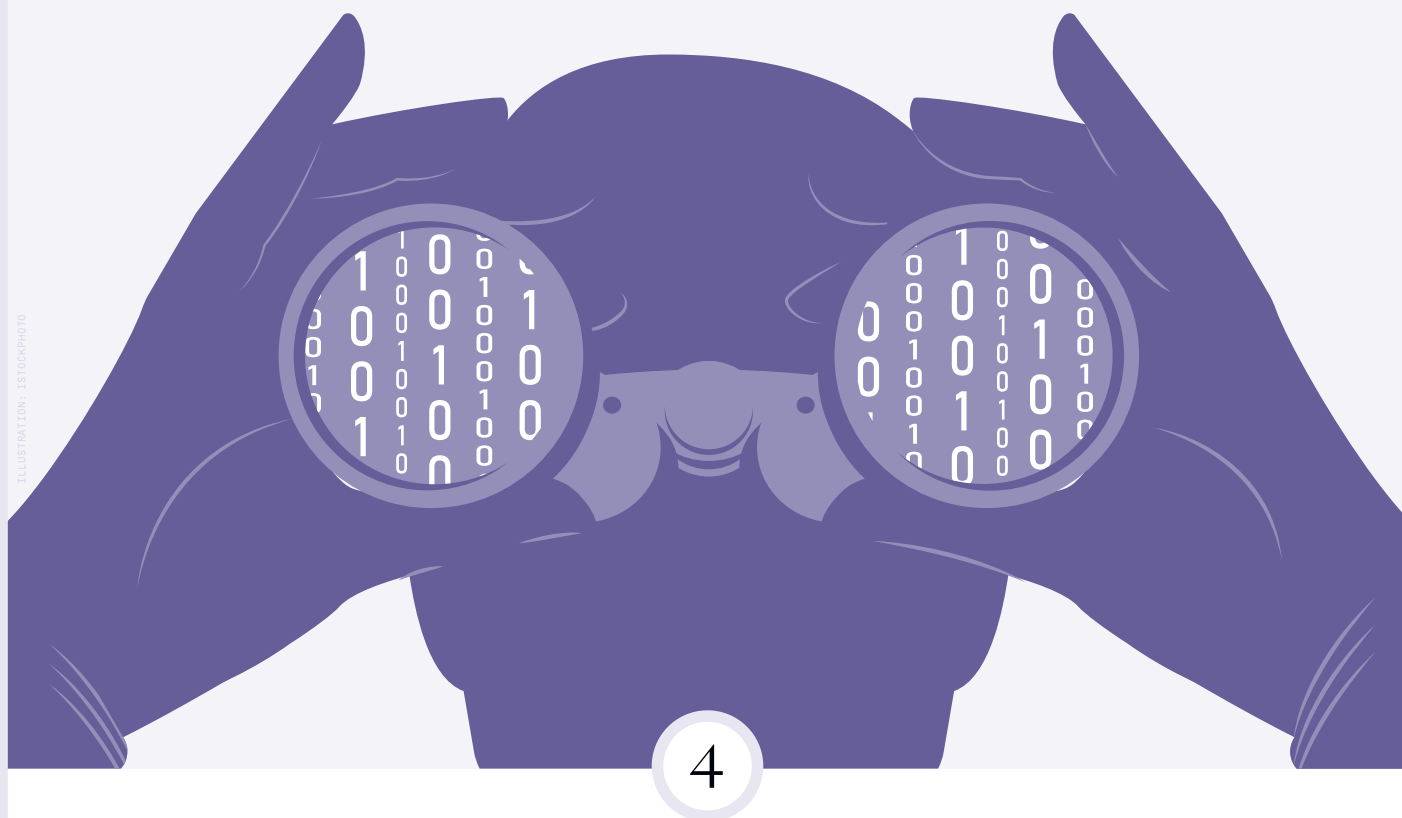
More awareness of cyberattacks

The number of cyberattacks is increasing, and this is reflected in this year's report. Those affected are found in all of the countries surveyed and in both small and large organizations.

At the same time, there seems to be a certain reluctance to talk openly about these events. Affected companies are afraid that it will reflect badly on their brand. However, there are clear examples of the opposite effect too: Those who share their experiences are perceived more positively than those who try to hide what has happened. Open discussion also helps everyone to learn from one another.

Resilience is about being flexible and being able to recover quickly after a potential incident. Threats must be detected and managed in a timely manner. This requires both technology and procedures to be put in place. It is essential for an organization to analyze risks, be aware of its own vulnerability, have a plan for unforeseen events, and, not least, train its personnel accordingly.

More organizations than last year state that they have a plan for unforeseen events such as cyberattacks, which is positive. However, too few seem to have tested their plan in practice, which is equally important. Most respondents say they have already adapted or will adapt their contingency plans to address cyberattacks. Worryingly, some have not done so or are not even intending to do so, despite a growing number of cyberthreats worldwide.

BUILDING RESILIENCE AND RESISTING THREATS

Cyberattacks are on the rise

Have you experienced any major cyberattacks in the last 12 months?

■ Public sector ■ Private sector

18%

78%

13%

83%

■ Yes
■ No
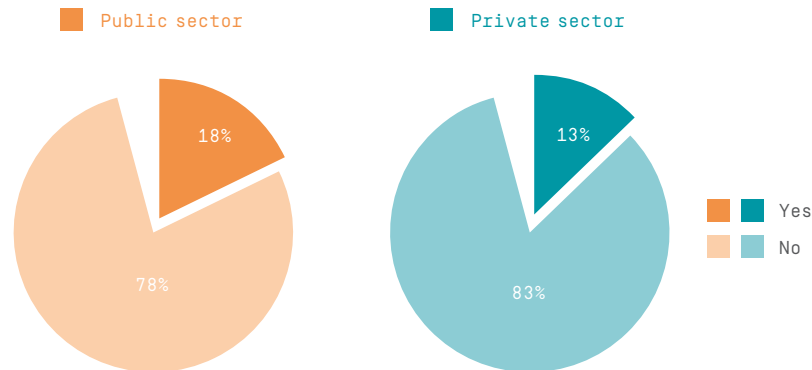
15 percent of IT decision-makers in the Nordic and Baltic regions have experienced major cyberattacks in the last 12 months. Those affected come from various countries and from both small and large organizations, relatively evenly distributed between the public and private sectors. However, the proportion is significantly higher in the Baltics (26 percent).

The interpretation of the term "major cyberattack" may vary among the respondents. There are indications that smaller, unsuccessful cyberattacks have also been included. This highlights the rise in intensity of cyberattacks, rather than pinpointing whether they have been disruptive or not. This might explain why the proportion of those affected is higher than in other surveys.

There also seems to be a certain reluctance to answer the question of whether or not the organization has been hit by a major cyberattack, which reveals a resistance to discussing the issue openly. Companies affected by a cyberattack are probably afraid of being depicted in a bad light. EU regulations make it mandatory to report incidents to the authorities within a certain timeframe, but this does not always result in general transparency toward the public or other organizations. However, experience shows that organizations willing to share their experiences openly are perceived more positively than those who

keep it secret, and this benefits their brand.

Cyberattacks have quickly become one of the most significant threats and their numbers are increasing. In the third quarter of 2024, cyberattacks in Sweden rose by 165 percent, which is the largest increase in Europe according to the news site Voister ("Cyberattacker mot Sverige ökar mest i Europa"). Security is improving, but it is a constant tug-of-war between good and evil. Technological advances are one thing, but it is often the human factor that is behind the success of a cyberattack. This highlights the importance of not just having a contingency plan, but also putting it into practice (see page 25).

BUILDING RESILIENCE AND RESISTING THREATS

More contingency plans, but few put to the test

Do you have a plan to deal with unforeseen events (e.g., cyberattacks) and do you know what is expected of you?

Public sector — 2025, 2024

Private sector — 2025, 2024

1. Yes, we have a plan.
2. Yes, we know what is expected of us.
3. Yes, we have practiced our plan.
4. No, we don't have a completed plan.
5. No, we don't know what is expected of us.

Multiple-choice question
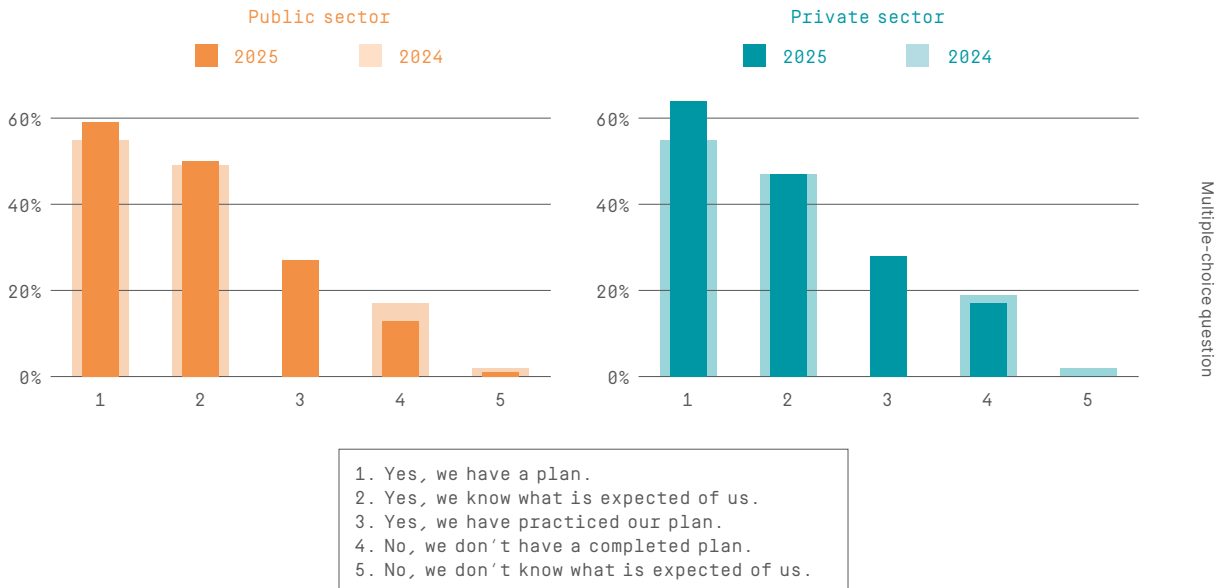
Compared to the 2024 report, the proportion of organizations that have a plan for how they will handle unforeseen events has increased, from 55 to 62 percent. The largest rise has been seen in Sweden, from 42 to 60 percent. In the Baltics, however, this figure has dropped from 60 to 50 percent.

The overall result indicates a shift in general understanding of the need for a contingency plan. At the same time, only 27 percent have actually tried out their plan. A contingency plan is not really complete until the organization has practiced executing it. There is a big difference between practicing the plan in isolation within the IT department and involving the corporate management as well to ensure resilience capability across the board. To maintain, develop, and test the organization's ability to handle an incident, it is important to practice the planned procedures, both within the organization and in collaboration with others. Practicing also offers an opportunity to identify any shortcomings in the plan, which may not become apparent until it is implemented.

The most prominent example of this is Denmark, where 38 percent of the respondents have practiced executing their plans, while at the other end of the scale is Sweden, where only 21 percent have done so. There is a heightened awareness in Denmark due to major incidents such as the 2023 ransomware attack on CloudNordic and the 2024 TDC Net outage.

In Finland, the proportion of IT decision-makers who know what is expected of them in the event of an unforeseen event is significantly higher than average, at 58 percent compared to 49 percent. The proportion of respondents who have no plan at all is also significantly lower in Finland. There are both geographic and historical aspects to this. Finland's proximity to Russia naturally has an impact and its National Emergency Supply Agency has a long history dating back almost a century. This has found its digital successor in Digipooli, which develops and supports preparedness in the ICT sector.

Laws and regulations drive security measures

Have you changed or do you plan to change your preparedness for cyberattacks?

Public sector — Private sector
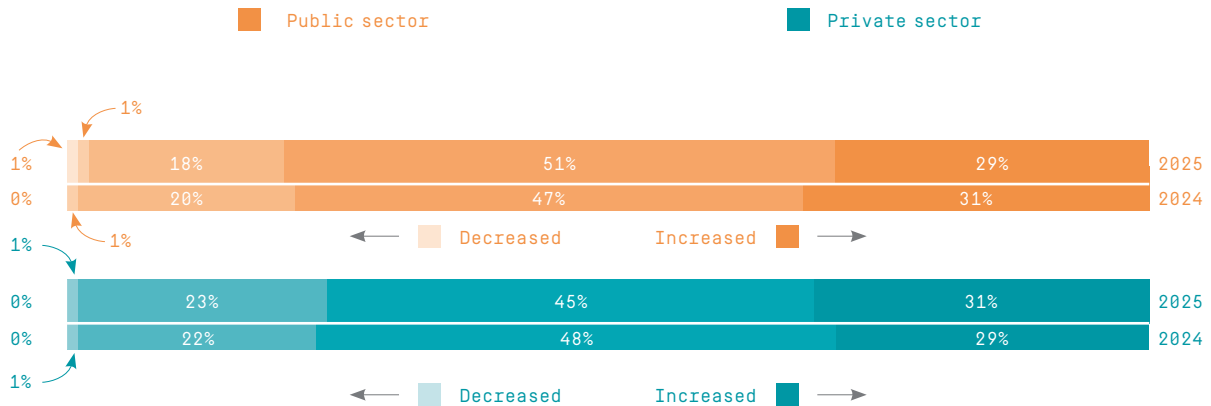
Almost half (48 percent) of IT decision-makers in the Nordic and Baltic regions say that laws and regulations are their top priority when it comes to planning security work. This opinion does not differ much between countries. The same applies to cyber threat intelligence, which comes in second place.

Laws and regulations are a significant driving force behind security measures. The NIS2 Directive, intended to establish a minimum level of cybersecurity in the EU, is currently an important issue and many organizations are struggling to meet its high requirements. There is some frustration that the regulations do not present any direct solutions and that there is a lack of precedent, which can make it difficult to interpret

the regulatory provisions. In Norway, the proportion of IT decision-makers who prioritize laws and regulations is not quite as high as in other countries. This can probably be explained by the fact that Norway is not part of the EU, so NIS2 is not yet a clear element of Norwegian legislation.
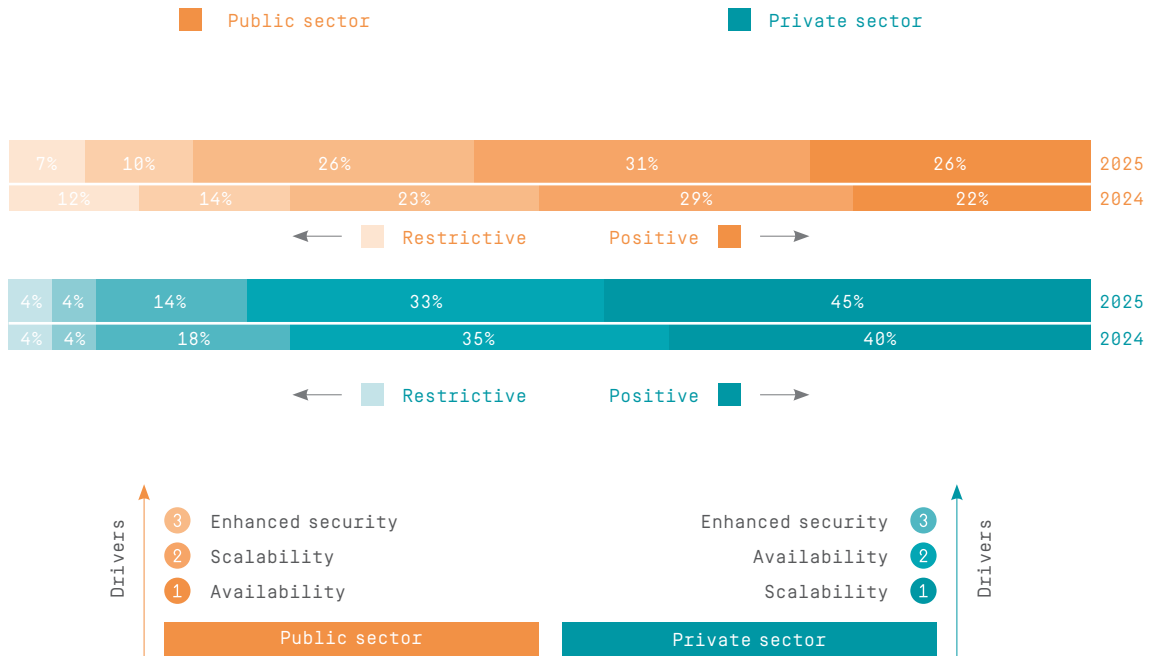
78 percent of the respondents have either adapted or are intending to adapt their contingency plans for cyberattacks, which means they reported an increase in preparedness (4 or 5). Despite rapidly increasing threats, not least due to the use of AI, 22 percent say they have not done so or do not intend to do so, which corresponds to a decrease in preparedness(1 to 3) or no change —which is remarkable. Not seeing cyberattacks as an equally disruptive

force as other organizational crises can perhaps be explained by the maturity level of the organization. Most organizations have not yet been attacked themselves. Organizations that have their own experience of cyberattacks tend to already have a plan in place and are also in the process of fine-tuning it. Compared to last year's report, looking at all countries combined, there have not been any notable changes in how organizations plan to change their preparedness for cyberattacks. Many organizations have plans for how they will handle different types of crises, but the IT element is often missing. In cases where plans exist, testing them out in practice is also key to ensuring their success (see page 25).

More organizations have a positive attitude toward public cloud solutions

What is your organization's current attitude toward using public cloud solutions?

■ Public sector ■ Private sector

7%	10%	26%	31%	26%		2025
12%	14%	23%	29%	22%		2024

← Restrictive   Positive ■ →

4%	4%	14%	33%	45%	2025
4%	4%	18%	35%	40%	2024

← Restrictive   Positive ■ →

Drivers
3 Enhanced security
2 Scalability
1 Availability
Public sector

Enhanced security 3
Availability 2
Scalability 1
Private sector
Drivers

The attitude toward public cloud solutions has moved in a positive direction, in both the private and public sectors. The number of respondents who say they are very positive has increased by five percentage points since last year, from 32 to 37 percent. The public sector is still somewhat more cautious. On the other hand, that is where the positive ranking (values of 4 and 5) has increased the most, from 51 to 57 percent, and also where the negative ranking (values of 1 or 2) has decreased the most, from 26 to 17 percent. This indicates that a shift in position among public organizations is a factor driving the general rise in positive attitudes toward public cloud solutions.

Security aspects as the biggest barrier have increased by six percentage points compared to last year. The biggest barrier in the private sector is security aspects (56 percent), while in the public sector it is legal uncertainties (70 percent) (read more about security focus on page 8). Sweden stands out in that 84 percent of public organizations there rank legal uncertainties as the biggest barrier to the acceptance of public cloud solutions. This can mainly be explained by uncertainty as to whether current agreements uphold sufficient trust to ensure proper data protection in line with GDPR requirements. Obstacles to using public cloud solutions vary between the countries where legal uncertainty and security are the main barriers. The common mindset in the Swedish public sector is a fear of doing something wrong, hence the inclination toward choosing a less risky path.

Scalability is the main driving force behind using public cloud solutions, except in the Baltic countries, which put availability first. Due to the political situation and the war in Ukraine, it has become increasingly important to be able to offload backups outside Lithuanian territory or to have a secondary site for production.

BUILDING RESILIENCE AND RESISTING THREATS

New regulations and technology help Länsförsäkringar strengthen it's resilience

Länsförsäkringar is a financial powerhouse with products in insurance, banking and pensions. With a strong physical presence in all of Sweden's counties, the company group aims for a matching digital presence that meets customers' expectations. At the same time, efforts are put into digital operations resilience to keep up with increasing threats and risks.

Maria Lundberg, Chief Digital Officer, Länsförsäkringar.

"In our 2033 plan we have defined areas for how our business will develop and how we can deliver increased value for our customers. My focus is to accelerate our abilities and technical skills but also develop the operational model: How do we get the job done," says Maria Lundberg, Chief Digital Officer at Länsförsäkringar.

Among the company's more than 4 million customers, far from all use the full range of services, a business opportunity that requires the company to meet the customer at the right moment with the right offer.

"We need to be both personal and relevant in our customer encounters. Therefore we run major initiatives to strengthen our tech capabilities, customer experience service offering, and data management. We have high ambitions in data, AI, and automation to level up our performance in a way that is ethical, compliant, and aligned with customer preferences."

For Maria Lundberg, the AI revolution is not mainly about applying technology but about change management and business development.

"Continuing working in the same way with the support of AI and automation will not lead to major

efficiency gains or bring competitiveness. Instead, we must use technology to work differently. Technology is 30 percent; the rest is innovation and change management."

Used correctly, technology will also support compliance management and adherence to new regulations and legislation.

"We are launching new AI features that give the employees the opportunity to chat with our own documents about, for instance, security guidelines and instructions. This way, everyone can more easily get the correct understanding of what applies and how to act, which becomes effective and safe, and increases our ability to be compliant."

Automation and AI will also be used in code generation and system development to enforce architecture

and security controls and procedures in the development process.

"It's a great opportunity to make security and compliance something that is not handled separately but is built in from start."

Attack attempts and fraud are increasing within the financial sector. Here, the Dora regulation has helped Länsförsäkringar set a clear focus and take measures to secure resilience and new competence.

"To level up our digital operational resilience we have implemented new tools and built a stronger technical expertise. As threats increase, we must push the development of our capabilities just as hard."

Extended risk analyses are also performed related to the geopolitical development and rising risk scenarios.

"For example, we have analyzed our suppliers, influence and contract periods, and the independence of European companies that have American parent companies."

Thanks to Dora, Länsförsäkringar could quickly overview and estimate risk in their supplier landscape.

"With the recent walkthrough of processes and supplier agreements, we are better equipped than a year ago to more quickly make the right decisions and take actions if needed."

More and more organizations are entering the world of AI

ILLUSTRATION ISTOCKPHOTO
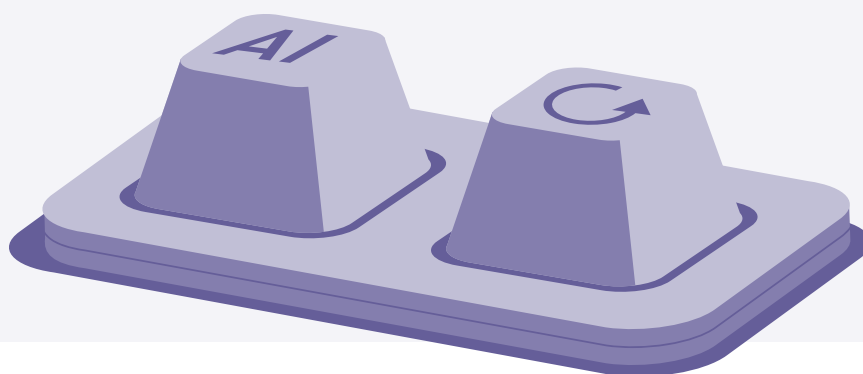
Artificial intelligence (AI) development is moving at breakneck speed, and more and more IT decision-makers in the Nordic and Baltic regions say they are using this technology in their production operations and intend to utilize it even more. This could bring great value to organizations.

An organization's AI journey is usually divided into five levels: beginner, explorer, practitioner, professional, and creator. More organizations are now seeing themselves as explorers and practitioners, while fewer rate themselves as beginners. A relatively large proportion also place themselves at the highest level as creators. Yet few organizations believe they have created significant value with the help of AI. This may be due to the fact that many have so far only implemented AI tools that make work more efficient for individual employees, but rarely at the organizational level—which is the only scenario where investments begin to yield real returns. An organization at the top end of the maturity scale should
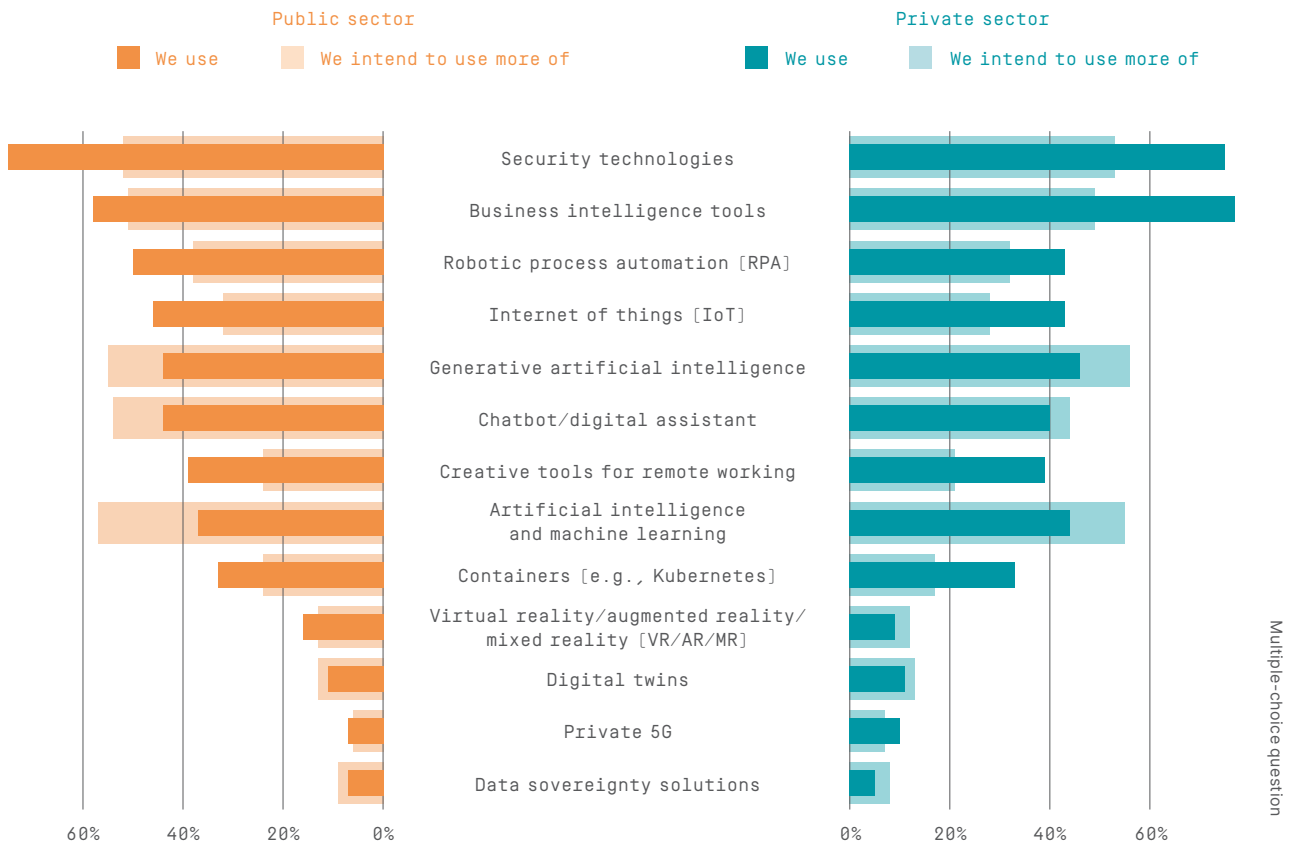
reasonably be expected to have already reached that point. This may indicate that many organizations have failed to integrate AI into their core processes.

One possible explanation for why organizations consider themselves to have shifted up the maturity scale may be a more structured approach to enabling end users to use generative AI solutions as part of their daily work. Focusing on the gains at the individual level but not being able to integrate AI into more general parts of the business processes reflects the AI maturity level of the organization. There is more to it than generative AI: There is also great potential offered by other AI technologies, which have been available for years.

Implementation of generative AI has almost doubled —and is expected to increase further

Technologies we use in production and intend to use more of within the coming three years:

Public sector
- We use
- We intend to use more of

Private sector
- We use
- We intend to use more of

Categories:
- Security technologies
- Business intelligence tools
- Robotic process automation [RPA]
- Internet of things [IoT]
- Generative artificial intelligence
- Chatbot/digital assistant
- Creative tools for remote working
- Artificial intelligence and machine learning
- Containers [e.g., Kubernetes]
- Virtual reality/augmented reality/mixed reality [VR/AR/MR]
- Digital twins
- Private 5G
- Data sovereignty solutions

Multiple-choice question

There has been a lot of public discussion about artificial intelligence (AI) agents and how they will revolutionize the way we work. This dynamic software performs data science tasks autonomously and interacts with its environment, setting it apart from traditional automation tools, which follow predefined rules. AI agents are believed to accelerate AI usage as they are expected to provide a good return on investment (ROI) in the form of high automation. Success for generative AI could also help provide a boost for other areas of AI, such as machine learning (ML) and natural language processing (NLP).

The growing interest in generative AI is clear. In 2024, 28 percent of IT decision-makers in the Nordic and Baltic regions stated that they had implemented generative AI in their operations. This year, the corresponding figure is 45 percent. 56 percent also

plan to use it more and an equal proportion intend to invest more in other AI technologies and machine learning. This means that these technologies are at the top of the list of technological tools that IT decision-makers intend to make more use of, closely followed by security technologies (53 percent). AI adoption is greater in organizations that consider themselves proactive in responding to business needs (see page 13). However, only a small percentage say they have created significant value with AI (see page 33).

Business intelligence (BI) is more commonly used in the private sector than in the public sector (77 percent compared to 58 percent). The interest in BI platforms can be correlated with the growing interest in generative AI solutions. These solutions can bring great value to organizations. BI tools that use AI and ML can create a system so smart that it knows of its own accord what

data should be used, so processes can be executed without the user having to input data.

In Denmark, robotic process automation (RPA) stands out in the public sector, with 75 percent of Danish public-sector respondents saying they use this technology, compared to 49 percent in the private sector. This country was an early adopter of RPA in public services and has strong government support for automation technology. The Danish Digital Agency has been instrumental in promoting strategic investments in AI and RPA technology, ensuring that public sector organizations have the resources and infrastructure needed to implement these solutions effectively.

Business needs and business value are generally ranked as top priorities when it comes to investing in new technology. Cost and ROI also rank high on the list.

Clear increase in AI maturity

How do you rate your organization's AI maturity?

Public sector
2025   2024

Private sector
2025   2024
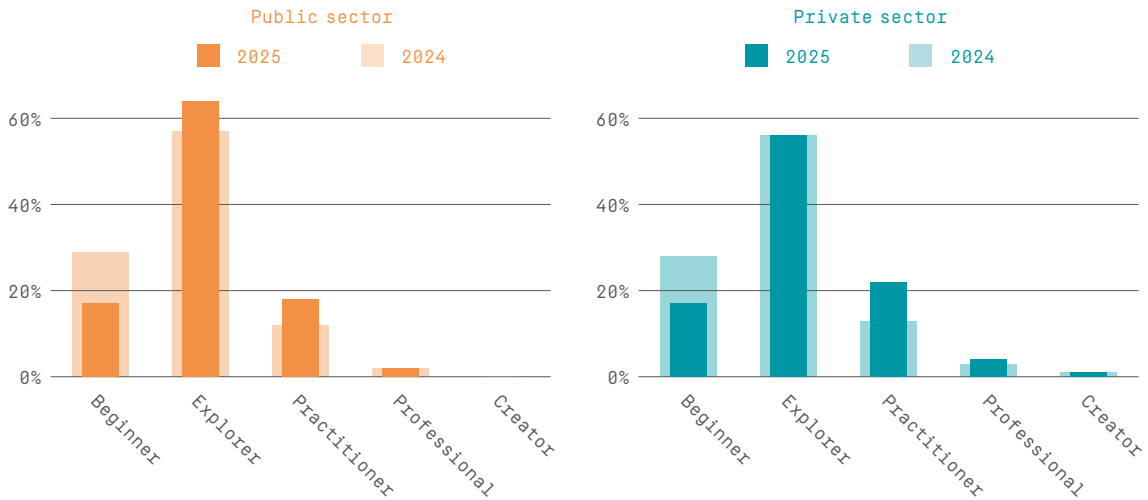
The majority (59 percent) of IT decision-makers see themselves as explorers (with a desire to start experimenting with AI and the first prototypes built) when it comes to artificial intelligence (AI). At the same time, it is clear that AI maturity has increased significantly since last year. 28 percent saw themselves as beginners in 2024, while the corresponding figure this year is 17 percent. Explorers were at 57 percent last year, while practitioners (with an AI vision established and a systematic approach started) have gone from 12 to 20 percent. Significant investments are being made in AI in both the private and public sectors, which is also starting to show in how the technology is being implemented. 15 percent of respondents in the private sector and 9 percent in the public sector strongly agree that AI creates substantial value (see page 33).

Overall, AI maturity is somewhat higher in the private sector, where 27 percent consider themselves to have reached the practitioner level or higher (professional or creator), compared to 20 percent in the public sector. This is likely due to the fact that public sector organizations handle more sensitive personal data, which entails greater legal constraints. The primary obstacles for the public sector are security constraints, regulatory uncertainty, data management, and talent availability, while the private sector is mainly concerned about data management and end-user upskilling.

Businesses that rank themselves as AI practitioners or higher are mainly in the private sector. These also use other technologies to a significantly greater extent, such as robotic process automation (RPA), container-based systems, and advanced remote work solutions (see page 30).

Few organizations are utilizing AI effectively

My organization has created substantial value with AI
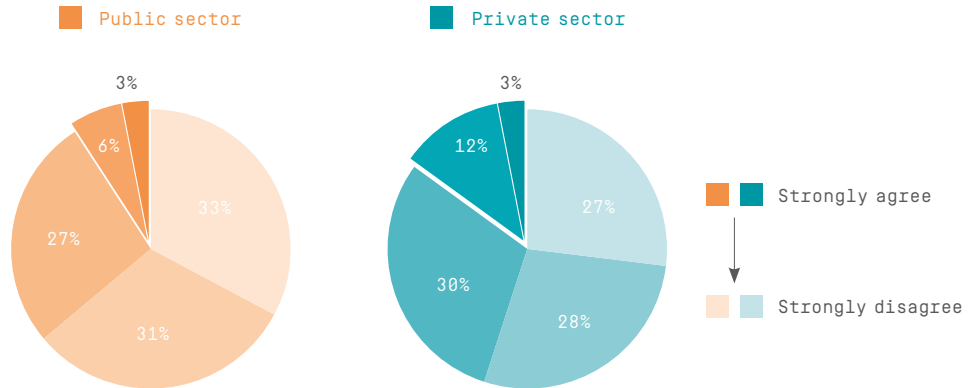
Although 59 percent of IT decision-makers see themselves as explorers in the field of artificial intelligence (AI), fewer now rate themselves as beginners and more regard themselves as practitioners (see page 32). Few believe they have created substantial value with AI so far. Only 13 percent answered "agree" or "strongly agree" to this question. 29 percent strongly disagree that AI has created substantial value, and in the Baltics this figure is even higher at 43 percent.

In many ways, this result is not unexpected considering that so many organizations are at the early stages of AI maturity. Content creation aids, internal chatbots, and similar tools are useful but do not necessarily generate major business benefits.

These are also the solutions that most IT decision-makers at the higher end of the scale (practitioner or higher) in the Nordics and the Baltics are using AI for, with content creation at the top of the list (62 percent). In Finland, the corresponding figure is as high as 78 percent. These AI workloads are common to start with, as they are readily available and can be used at an individual level to increase the productivity of individual employees. The results suggest that many organizations, despite viewing themselves as practitioners or higher, have not yet moved beyond this basic level.

Over time, the focus tends to shift to other, more value-enhancing processes at the organizational level. A significant return on investment (ROI) can only be expected when

AI is integrated into the organization's core processes and used to support reactive and predictive decision-making and create new products and services based on available data. The expected development in using AI agents would be a major step in that direction.

Many organizations appear to have failed to integrate AI into their core processes. Generative AI may be the newest and most talked-about technology, but there is a great deal of untapped potential in other AI technologies that have been available for several years. Respondents who consider themselves to have gained significant or very significant benefits from AI are also much more likely than others to have used AI for customer service and process automation.

TECHNOLOGIES AND TRANSFORMATION FOR THE FUTURE

Navigation meets intelligence

In the maritime industry, it's no longer just about compasses and charts—it's algorithms, real-time data, and artificial intelligence that are steering the course for NAVTOR, a cutting-edge technology company based in Egersund, Norway.

Anders Holme, CTO, NAVTOR.

NAVTOR develops digital solutions for the global shipping industry, currently used on over 18,000 vessels worldwide. The company has positioned itself as a key player in the maritime tech space with a clear mission: To make navigation smarter, decision-making better, and operations more efficient —all through the power of artificial intelligence (AI).

AI in action—already in use
"We're using AI to optimize routes and predict maintenance needs. This leads to better decisions, lower risk, and saves valuable time," says Anders Holme, CTO at NAVTOR.

AI isn't something they're just testing—it's already fully operational. A prime example is their vessel traffic monitoring system, which constantly analyzes large volumes of data and provides real-time decision support to operators.

The system learns over time and recommends the most efficient routes based on a combination of machine learning, validated maritime data, and human expertise.

The result? Faster decisions, fewer deviations—and greater control for ship owners.

Digital twins offer full insight
AI is also used to develop digital twins of ships—virtual models that allow operators to simulate various operating conditions. When combined with AI, these models open up a world of new possibilities:

"Through these models, we can predict fuel consumption and CO_2 emissions under different weather conditions, enabling smarter route planning," says Anders Holme. "These simulations help optimize operations, reduce wear and tear, and allow proactive action—long before issues occur."

NAVTOR has set an ambitious goal of reducing CO_2 emissions from shipping by up to 20 percent —a target Anders Holme says is fully achievable with today's technology.

"We believe technology and sustainability go hand in hand. Our systems give shipping companies real-time insight into their CO_2 output and fuel use. It's not just good for the planet—it's smart business," he adds.

AI as a digital defense
AI also plays a key role in NAVTOR's cybersecurity efforts. Ship control systems are increasingly vulnerable to digital threats, and AI is central to strengthening their defense.

"We use AI to monitor unusual activity and alert operators to potential threats in real-time. It's about protecting both data and operations," says Anders Holme.

With increasingly complex onboard systems, security is a prerequisite for digitalization—and AI is proving to be a powerful tool in this area.

The future of shipping has already begun
With a strong focus on AI, digital transformation, and sustainability, NAVTOR is well positioned to lead the shipping industry into the future. The technology being developed in Egersund is setting a new standard for how maritime companies can tackle efficiency and environmental challenges.

"We develop technology that provides our customers with simpler and smarter solutions to meet the challenges and sustainability goals of the future. This is the essence of modern shipping," Anders Holme concludes.

The future is in our hands

As 2025 continues, one of the most important tasks of an IT decision-maker will be to make sure the roadmap is thoroughly outlined and well communicated: Even though IT must take the lead, no one will succeed on their own.

Everyone in the organization needs to understand where you are going, and why. Responsibilities need to be clearly defined, and everyone must be on board with the priorities. The future will demand change, growth, and courage from all of us.

Strategies have to involve both business processes and people. One does not work without the other. Efforts must be put into communication skills, and investments in competence development will be necessary. IT decision-makers have to make sure everyone has the ability and resources needed to contribute on the path forward.

The digital transformation must follow your roadmap yet be adaptable to global events and unforeseen turns. IT departments must act both as a support function and a leading star, while translating goals and missions into cost-efficient tools and technological solutions.

Security continues to be essential as we steer through the implementation of new technology, robust frameworks, and a rapidly changing political climate. This requires organizations to both increase the security understanding at large and become better at transferring knowledge internally.

Again—processes and people at heart.
Finally, we must continue to learn from the past and the present. The report in your hands represents one way of doing so. A lot is in our hands and together we can take giant leaps as leaders, organizations, and countries, all while building an even stronger northern region.

59%

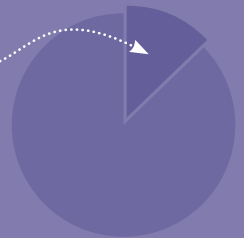do not act proactively towards
the business's needs.

69%

will increase their
spending in security.

#1

biggest obstacle to AI
is data management.

Only
13%

have created
substantial value
with AI.

23%

AI practitioners
and professionals.

2025

2024

CIO ANALYTICS

2025