GlobalConnect IT Insights:

Cybersecurity

Risks and resources from the IT leader's perspective

GlobalConnect

Contents

About the survey

The survey was conducted by Demoskop on behalf of GlobalConnect. Data collection was carried out using a mixed method combining qualitative and quantitative elements through telephone interviews.

The target group consisted of IT-Managers and Security leaders operating at a Nordic and/or national level in companies with 150 or more employees active in the markets of Sweden, Norway, and Denmark.

A total of 225 telephone interviews were conducted (75 interviews per country) during the field period of September 3–20, 2024.

Preface:

Are Scandinavian IT leaders prepared for today's cyber threats?

Several reports show that cyberattacks are increasing globally at an ever-faster pace. Cybercrime has evolved into a lucrative industry that rapidly adopts new technologies to achieve its own or a client's objectives – whether it involves industrial espionage, advancing the interests of state actors, or outright extortion.

But how do IT leaders themselves perceive the threat landscape and their ability to address it? Is it even possible to be fully prepared for today's cyber threats? To explore these questions and more, we at GlobalConnect enlisted the help of the research firm Demoskop.

More than 200 IT- and Security leaders across Sweden, Norway, and Denmark were interviewed.

The results present a complex picture. On one hand, IT leaders report a high level of security, yet on the other, they express concern about attacks and disruptions. Alarmingly, a significant proportion report that business-critical data is not securely stored, and that employees' security awareness is lacking.

In the following pages, you will find data and insights from the survey, as well as continuous commentary from GlobalConnect's own experts. Personally, I found it fascinating to observe the differences between our three Scandinavian countries, as well as the distinct challenges faced by the private and public sectors.

Happy reading!

Anna Granö, Executive Vice President for B2B at GlobalConnect

"The results present a complex picture. On one hand, IT leaders report a high level of security, yet on the other, they express concern about attacks and disruptions."

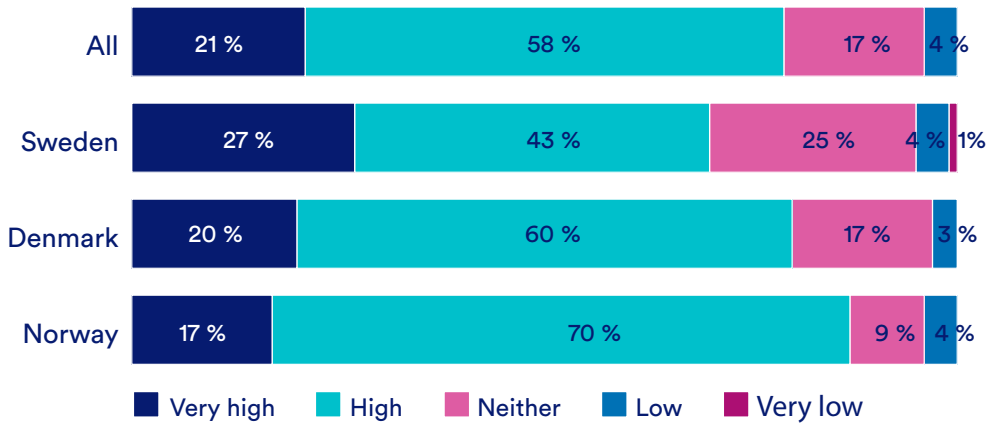
Part 1 - The current situation

8 out of 10 report a high level of security

The overall picture shows that IT leaders have a relatively high level of confidence in their organizations' security. Confidence is highest in Norway, where 87% of participants rate their security as high or very high. In Sweden, the figure is significantly lower, with only 69% sharing this positive view.

IT leaders in the public sector rate their security slightly higher than their counterparts in the private sector. Additionally, companies with the largest workforces and highest revenues express greater confidence in their security compared to smaller organizations.

How would you rate your current security level?



Private vs Public sector

	All	Private	Public sector
1. Very high	21%	28%	23%
2. High	58%	49%	60%
3. Neither	17%	17%	15%
4. Low	4%	5%	3%
5. Very low	0%	1%	0%

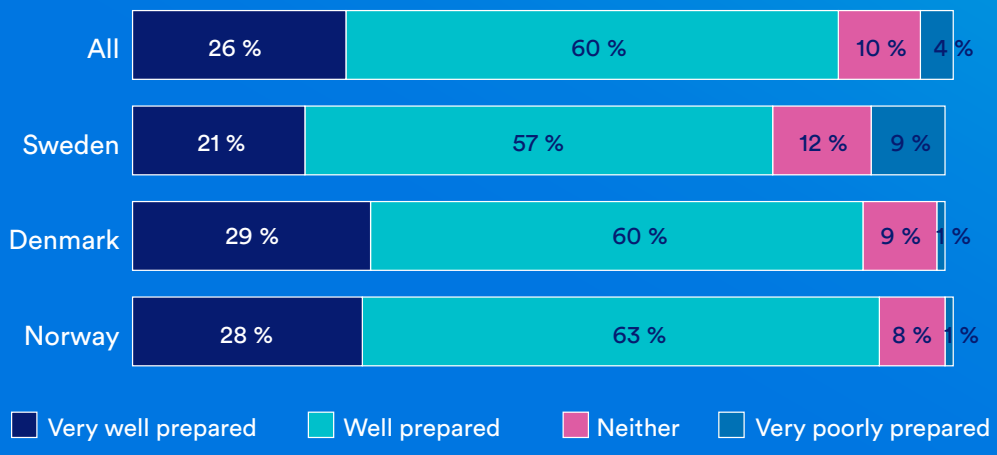
Company size

	Up to €57 million	€60–150 million	€160 million or more
1. Very high	19%	22%	25%
2. High	61%	52%	58%
3. Neither	17%	21%	13%
4. Low	3%	4%	4%
5. Very low	0%	1%	0%

86% are prepared to restore lost data

The ability to recover lost data after a cyberattack is a critical cornerstone of modern cybersecurity. In this area, too, IT leaders express confidence. Norway once again leads the way, while Swedish IT leaders are slightly more hesitant.

How prepared are you to restore lost data after an attack?



Expert commentary:

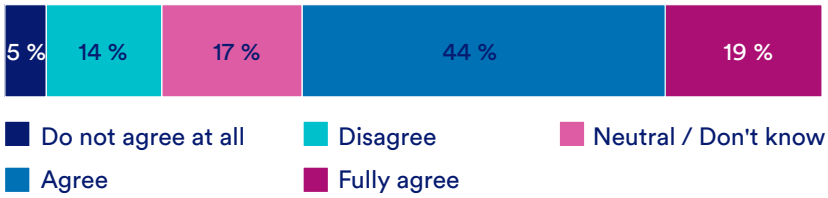
"It would be fantastic if security levels were as high as IT leaders report. Unfortunately, it's more likely that risks are underestimated and preparedness is overestimated. While organizations may have the capacity to restore lost data, budgets often don't account for the associated costs. On average, ransomware victims lose 35% of their data permanently."

Øystein Snekkerlien, Security Strategist, GlobalConnect

6 in 10 worry about IT attacks or failures

Concern about IT attacks or failures is highest in Denmark (83%) and lowest in Sweden (52%). Private sector employees are slightly more concerned than public ones. Among smaller businesses, 57% express worry, compared to 69% in the largest firms.

To what extent do you agree with the statement, 'We feel concerned about an IT attack or IT disruption'?



Private vs Public sector

	All	Private	Public sector
1. Do not agree at all		18%	20%
2. Disagree		49%	33%
3. Neutral / Don't know		15%	28%
4. Agree		12%	18%
5. Fully agree	5%	6%	3%

Company size

	Up to €57 million	€60–150 million	€160 million or more
1. Do not agree at all	16%	15%	33%
2. Disagree	41%	55%	35%
3. Neutral / Don't know	18%	15%	17%
4. Agree	19%	10%	10%
5. Fully agree	6%	5%	4%

Expert commentary:

"Public sector organizations are becoming aware that they are prime targets for cyberattacks. However, they often struggle to compete with private companies for top cybersecurity talent. We've seen an increase in attacks aimed not at economic gain but at destabilizing society, sowing fear among citizens, and eroding trust in public institutions. These attacks target IT systems linked to public services, such as water supply."

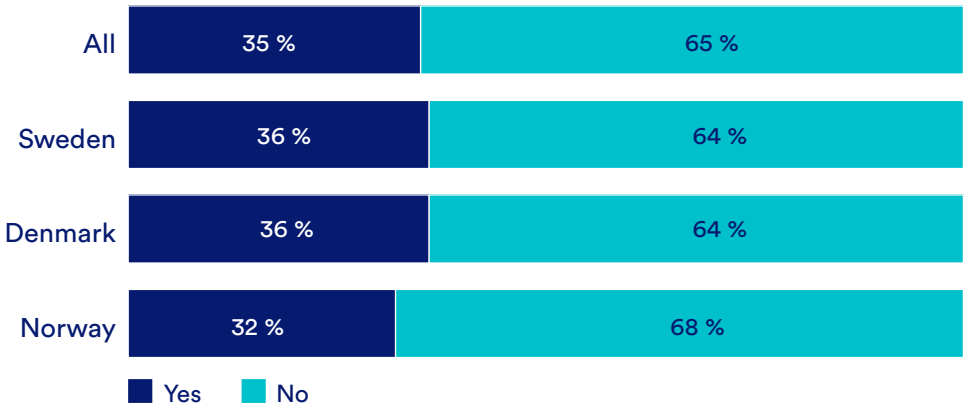
Uffe Traberg, Commercial Director, GlobalConnect

More than half of large companies have experienced IT attacks

Slightly more than one-third of participants report that their organization has been subjected to an IT attack in the past two years. The prevalence is slightly lower in Norway compared to Sweden and Denmark. Private sector organizations are somewhat more affected than those in the public sector.

The highest exposure is found among companies with the largest turnover. In the category with annual revenues of €160 million or more, 52% report having been attacked. This is noteworthy considering that IT leaders in this category are less worried about IT attacks and rate their security levels higher than their counterparts in smaller companies. Could it be that a high level of threats has become "the new normal" for these organizations, and they feel equipped to handle the situation they face?

Have you been subjected to an IT attack in the past two years?



Private vs Public sector

	Private	Public sector
1. Yes	35%	33%
2. No	65%	68%

Company Size

	All	Up to €57 million	€60–150 million	€160 million or more
1. Yes	35%	30%	29%	52%
2. No	65%	70%	71%	48%

Expert commentary:

"Despite the prevalence of cyberattacks and data breaches today, too many still think, 'It won't happen to us.' This mindset is particularly common in smaller companies, which, while rarely targeted by specific attacks, are at risk of falling victim to broad, automated ones. However, I believe we are witnessing a generational shift. Younger IT leaders are more aware of the risks than their older counterparts and are also more willing to admit they don't have full control—a challenging position to maintain given how rapidly the threat landscape evolves."

Emma Helton, Product Manager Cybersecurity, GlobalConnect

Part 2 – Risk factors undermining security

Risk factor 1:

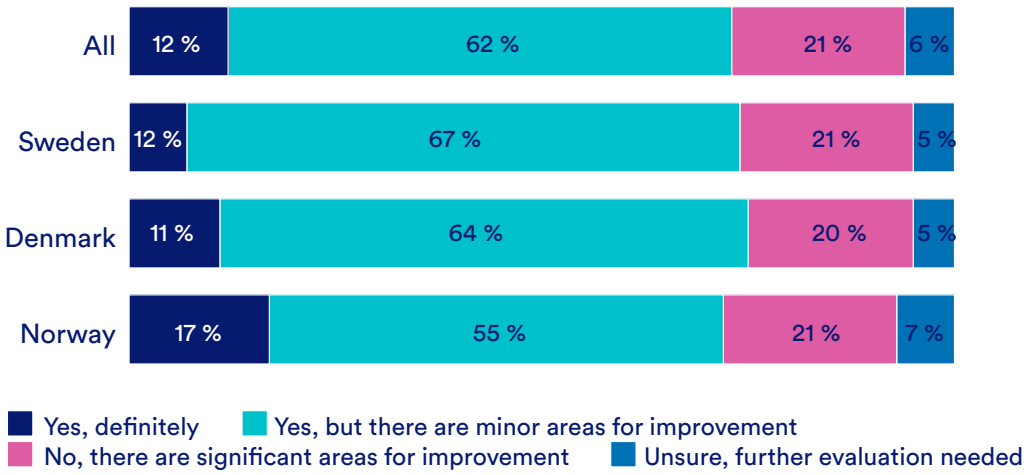
The digital infrastructure

1 in 5 see significant improvement needs in their IT environment

A well-planned and continuously updated IT environment is a fundamental requirement for maintaining high cybersecurity levels over time. Without this, there is a significant risk that attackers will exploit vulnerabilities, such as outdated systems that no longer receive security updates. According to the survey, as many as one in five respondents see significant improvement needs, while only slightly more than one in ten are fully satisfied with their current IT environment.

Norway stands out in this regard. A full 17% of respondents there report having the best possible IT environment, compared to 11% in Denmark and just 7% in Sweden.

Do you believe you currently have the best possible IT environment?

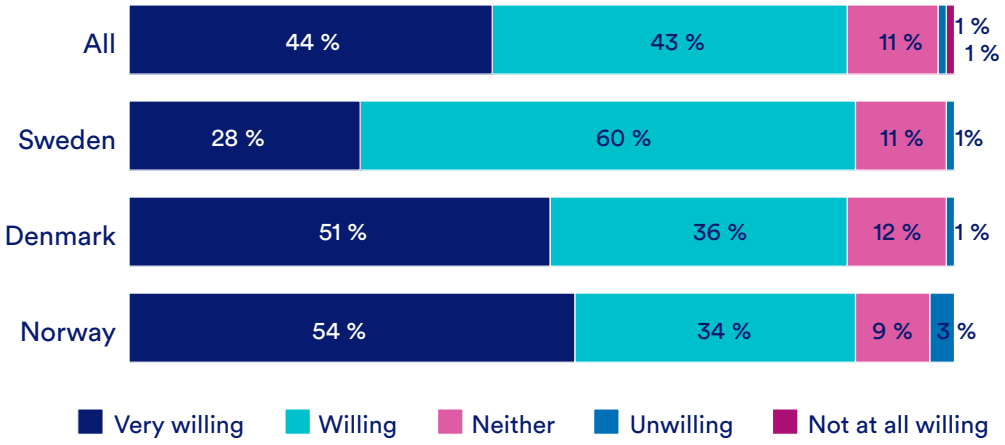


"1 in 5 see significant improvement needs in their IT environment"

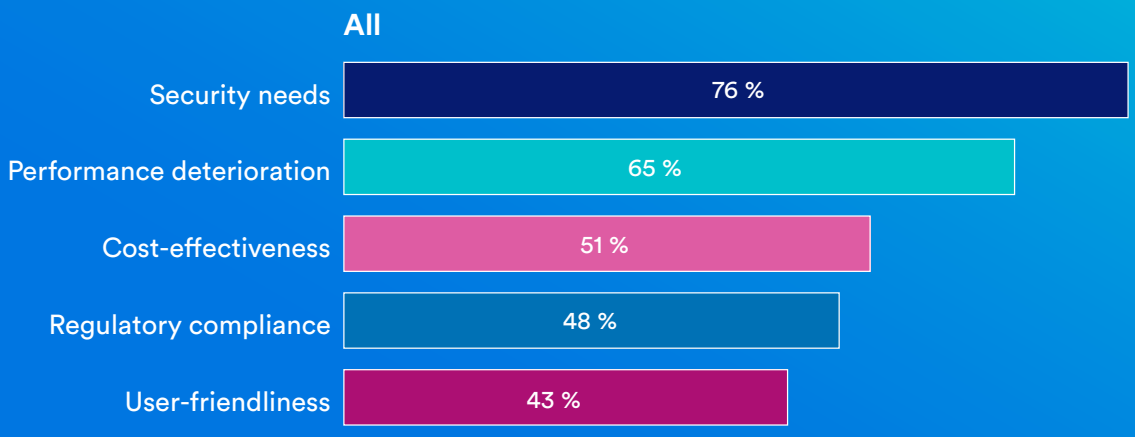
9 out of 10 regularly replace outdated IT components

A reassuring majority of IT leaders report that they are inclined or highly inclined to replace outdated parts of their IT environment. Security is cited as the primary reason for this practice, though performance, cost efficiency, regulatory compliance, and user-friendliness are also important factors.

How inclined are you to replace outdated hardware and expired licenses?



What are the primary reasons for replacing outdated technology and licenses?



Respondents were allowed to select more than one answer. Therefore, the columns do not necessarily add up to 100%.

Is the legacy challenge greater in the public sector than in private industry?

16% of IT leaders in the private sector believe they have the best possible IT environment, compared to only 5% in the public sector. Additionally, only 2% in the private sector report being uncertain and needing to further evaluate their situation, while this figure rises to 13% in the public sector.

The two sectors also differ in their willingness to phase out outdated IT components. In the private sector, 90% of respondents say they are inclined or highly inclined to replace old hardware and expired licenses, compared to 85% in the public sector.

That said, the public sector appears to perform better than the private sector in other critical security areas, which will be discussed in the upcoming sections.

Expert commentary:

"There's a built-in inertia in the public sector due to how budgets and procurement processes work. From recognizing a need to implementing a solution, the lead times are long, as extra funds must be requested, and a public procurement process must be carried out. In my experience, action is often delayed until the situation becomes critical, or until an existing supplier's multi-year contract expires. From a security perspective, this is a risky strategy."

Uffe Traberg, Commercial Director, GlobalConnect

12 % experience shortcomings in their security solutions

How much confidence do IT leaders have in the security solutions intended to protect their organizations from cyberattacks and breaches? While a majority report no issues with components such as firewalls and antivirus systems, there is clear room for improvement – especially in Sweden.

The percentage of IT leaders experiencing issues with their security solutions is higher in the private sector (15%) compared to the public sector (5%).

To what extent do you agree with the statement, "We have issues with deficiencies in security, such as firewalls, intrusion protection, and antivirus protection"?

	All	Sweden	Denmark	Norway
1. Fully agree	2%	3%	1%	3%
2. Agree	10%	12%	11%	8%
3. Neutral / Don't know	12%	21%	8%	8%
4. Disagree	44%	41%	47%	43%
5. Do not agree at all	31%	23%	33%	38%

Expert commentary:

"A clear trend in recent years is that cybercriminals don't break in—they log in. Compromised credentials are an underestimated security risk. These breaches are not detected by antivirus systems, allowing attackers to quietly extract the data they want. IT leaders need to take a broader approach to data security to address these risks effectively."

Øystein Snekkerlien, Security Strategist, GlobalConnect

Sweden performs worst in secure data storage

Nearly one in five IT leaders (17%) in Sweden report that their organizations have business-critical data that is not securely stored – a concerning result. The corresponding figures are significantly lower in Norway (9%) and Denmark (5%).

When comparing the private and public sectors, the contrast is less pronounced, but insecure data storage is more common in the private sector.

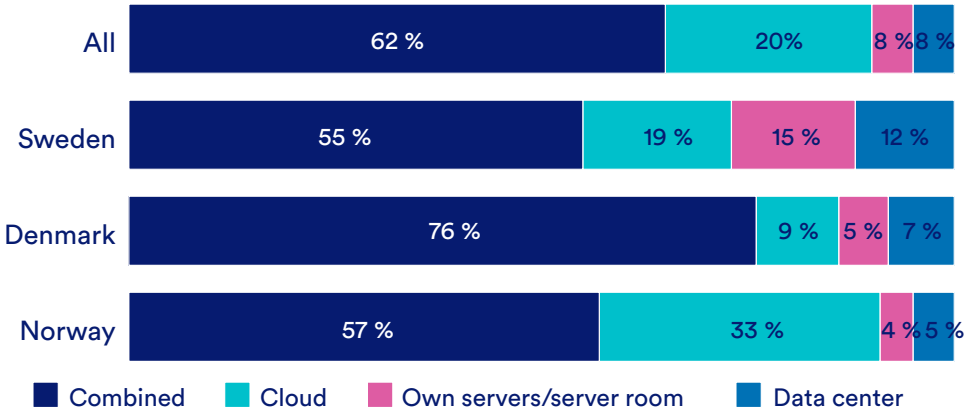
To what extent do you agree with the statement, "We have business-critical data that is not securely stored"?

	All	Sweden	Denmark	Norway
1. Fully agree	2%	3%	1%	3%
2. Agree	10%	12%	11%	8%
3. Neutral / Don't know	12%	21%	8%	8%
4. Disagree	44%	41%	47%	43%
5. Do not agree at all	31%	23%	33%	38%

Norway leads in cloud storage

The most common approach is to combine various storage methods. The highest proportion of organizations primarily using cloud storage is found in Norway (33%), while the lowest is in Denmark (9%).

How do you store data today?



Private vs Public sector

	All	Private	Public sector
1. Cloud	20%	16%	25%
2. Data center	8%	8%	8%
3. Own servers/server room	8%	9%	5%
4. Combined	62%	67%	58%
5. Other	1%	0%	5%

Expert commentary:

"Norwegian organizations have embraced cloud storage more than other countries, so it's not surprising that Norway stands out here. The question, however, is whether we will see a slowdown in this trend. Many are becoming aware of how costly it is to have cloud providers restore data after a breach. Geopolitical factors also play a role. In Denmark especially, we are seeing an increased demand for data storage within the Nordic region and the EU, rather than with cloud providers based in the US."

Øystein Snekkerlien, Security Strategist, GlobalConnect

Risk factor 2:

Employee knowledge

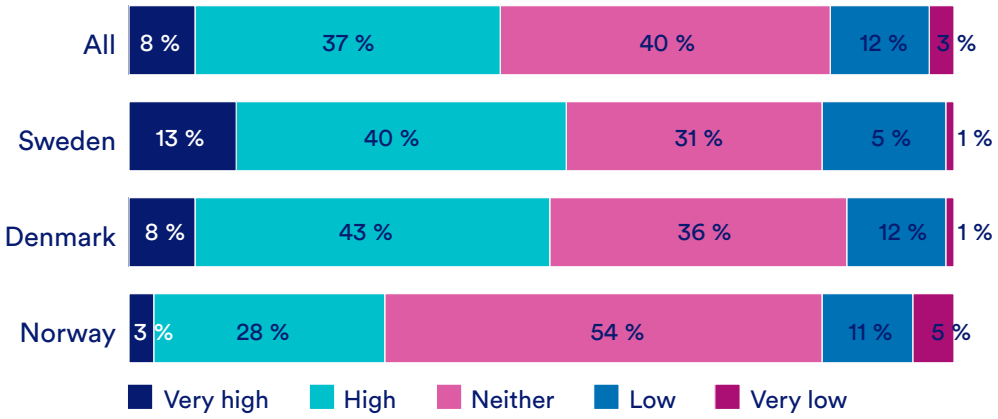
Less than half are satisfied with internal knowledge levels

It is often said that a chain is only as strong as its weakest link. Even with security solutions and protocols in place, they are of little value if employees do not use them correctly.

The human factor appears to be a vulnerability worth greater focus in the future.

IT leader's confidence in their employees is significantly lower than their confidence in the overall security level. Only just over half of respondents in Sweden and Denmark rate employees' cybersecurity knowledge as high or very high. In Norway, the figure is even lower, at just 30%.

How would you rate the level of knowledge among employees/ in the organization regarding cybersecurity?



Expert commentary:

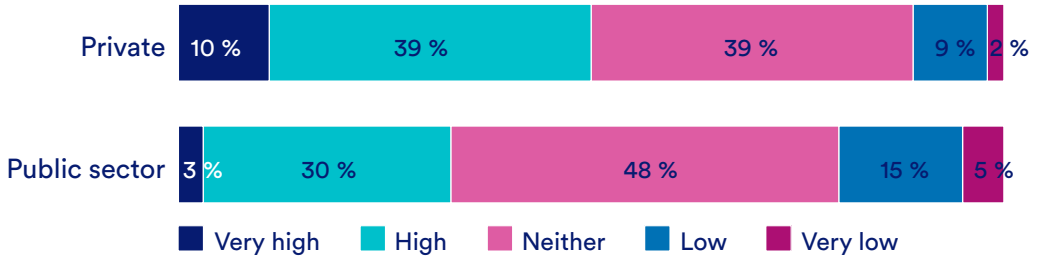
"Cybersecurity knowledge needs to extend beyond the IT department so that all employees understand how they can help mitigate risks. Equally important is designing your IT infrastructure to make it easy to do the right thing. If systems are too complicated, employees will find ways to bypass your security restrictions."

Øystein Snekkerlien, Security Strategist, GlobalConnect

1 in 5 public-sector IT leader's assess knowledge levels as alarmingly low

Knowledge levels also appear to vary between the private and public sectors. A full 20% of public-sector IT leaders rate employees' cybersecurity knowledge as low or very low, compared to 11% of IT leaders in the private sector.

How would you rate the level of knowledge among employees/ in the organization regarding cybersecurity?



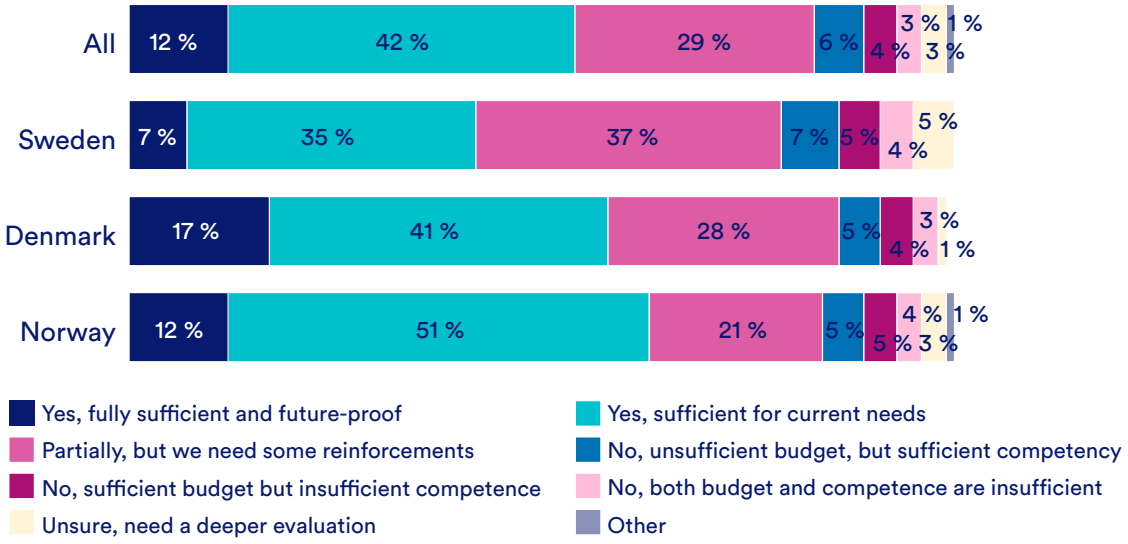
Risk factor 3:

Resources and authority

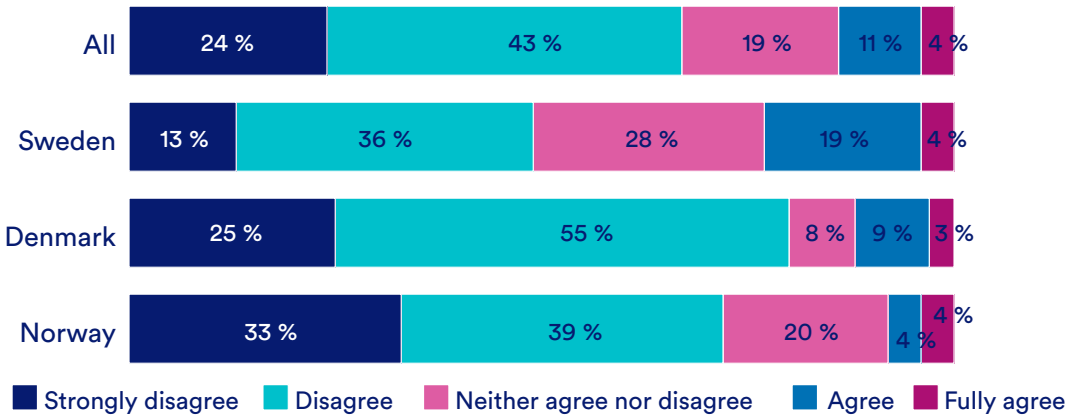
4 in 10 IT leaders require additional support to achieve desired security levels

Shortcomings in budget, internal expertise, or both prevent a significant proportion of IT leaders from maintaining the security level they believe their organization should have. Only slightly more than 1 in 10 report having sufficient resources to meet both current needs and future-proofing requirements. In Sweden, nearly one in four IT leaders state that they frequently encounter issues they struggle to manage with existing resources.

Do you currently have sufficient budget and expertise to maintain the security level your organization requires?



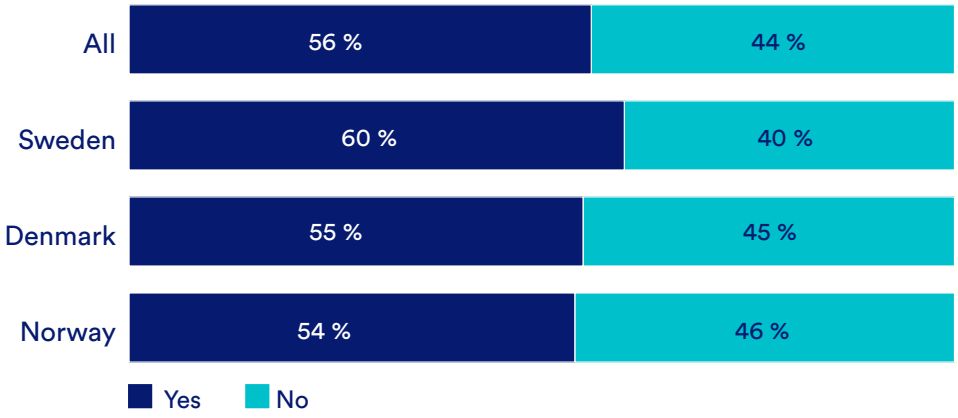
How much do you agree with the following statement: Problems related to IT or IT security arise far too often, which we find difficult to handle with existing resources?



A slim majority of IT leaders sit on the executive team

despite the strategically critical role IT plays today, it is still far from guaranteed that the IT leader has a seat on the executive team. The proportion is slightly higher in Sweden than in Norway and Denmark, and higher in the public sector compared to the private sector.

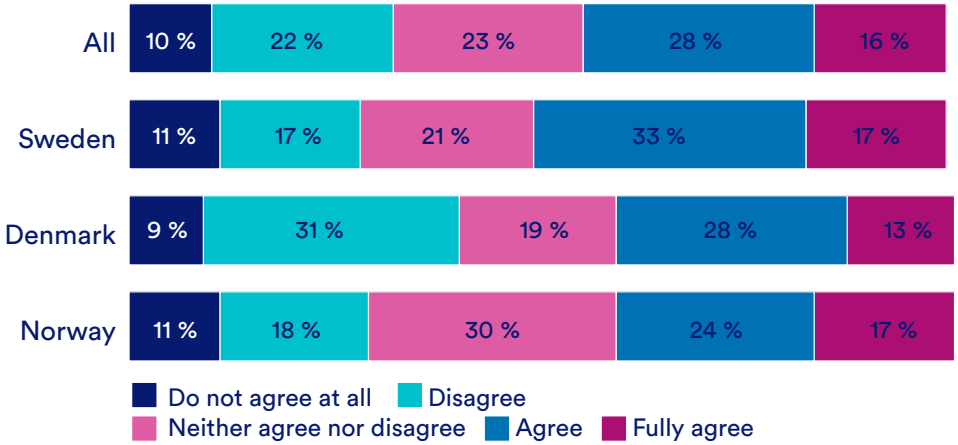
Is the IT leader a member of the management team?



45 % view leadership's IT competence as insufficient

approximately half of IT leaders believe that the executive team's IT competence needs improvement. Perhaps the first step is ensuring the IT leader has a seat at the table.

How much do you agree with the following statement: The IT competence of the management team is insufficient, considering how strategically important IT is today?



Conclusion: Cybersecurity is more than just an it issue

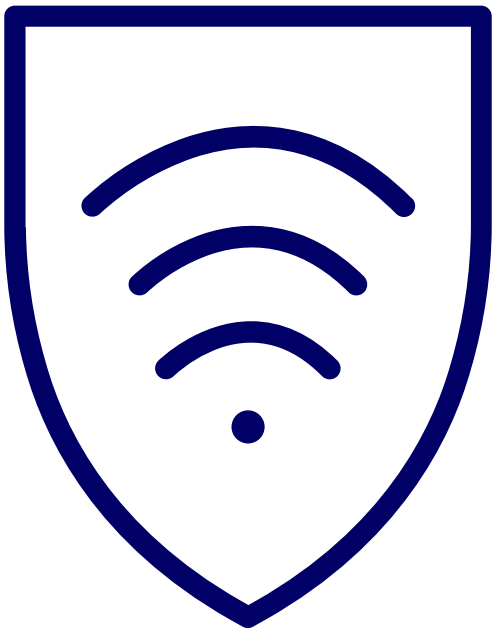
today's IT leaders face complex challenges when it comes to cybersecurity. Their role has never been more critical, given the increasing volume and sophistication of cyberattacks. However, our survey reveals that IT leaders too often lack the necessary resources and support to address the challenges they face.

A few years ago, GlobalConnect published a report aptly titled "The IT Manager's Impossible Mission." It highlighted the stress, overtime, and ever-expanding responsibilities IT leaders endure, often without corresponding increases in resources.

We now live in a global landscape marked by conflicts and polarization. Cyberattacks are rising at unprecedented speeds, impacting entire societies. Technological advancements in AI and quantum computing not only bring great opportunities but also introduce new risks. Despite this, the IT leader still does not have a guaranteed place on the executive team.

It is high time to stop viewing cybersecurity as solely an IT issue. A modern security strategy requires clear prioritization, anchored at the highest levels of leadership, and ingrained routines practiced by every employee.

Without this, organizations risk relying on isolated measures, like investing in a firewall or antivirus software, missing the continuity and holistic perspective needed to protect against both present and future risks.



About GlobalConnect

GlobalConnect is one of Northern Europe's leading providers of digital infrastructure and data communication. With a 235,000-kilometer fiber network spanning Denmark, Norway, Sweden, Germany, and Finland, we deliver fiber-based broadband services to over 830,000 private households and provide network solutions to approximately 30,000 B2B customers. This is how we keep society running and enable tomorrow's innovations.

GlobalConnect