GlobalConnect IT Insights

Public Sector

A status report on the opportunities, risks, and drivers for IT leaders in the public sector.

GlobalConnect

Contents

About the survey

The survey was conducted by Demoskop on behalf of GlobalConnect with 225 participants. The target group consisted of IT leaders and Security Managers at Nordic and/or national level from companies with 150+ employees operating in Sweden, Norway, and Denmark. This report is based on a selected subset of the total respondents, specifically those working within the public sector.

Data was collected using a mixed-method approach combining qualitative and quantitative insights through phone interviews. A total of 225 phone interviews were conducted (75 per country) during the period of 3rd-20th September 2024.

Preface

What is the state of IT in the public sector?

Without well-functioning IT infrastructure, there can be no well-functioning societies. So how digitally prepared are our public institutions for the opportunities and challenges of today and tomorrow?

We have partnered with research firm Demoskop to take the temperature of IT leaders in Sweden, Norway, and Denmark. In this report, we focus specifically on IT leaders in the public sector. How do their circumstances, challenges, and strategies differ from those of their counterparts in the private sector?

In the pages that follow, you will find insights and analysis from the survey, accompanied by commentary from our own experts. The report is divided into three sections, each with a dedicated focus: digital infrastructure, cybersecurity – and last but not least, the future, including developments in AI, quantum technology, and tightening regulatory demands.

I hope this report provides you with valuable insights to apply in your professional role – and sparks meaningful conversations both within and beyond your organization.

Enjoy the read!

Anna Granö, Executive Vice President B2B at GlobalConnect

Part 1:

The Digital Infrastructure

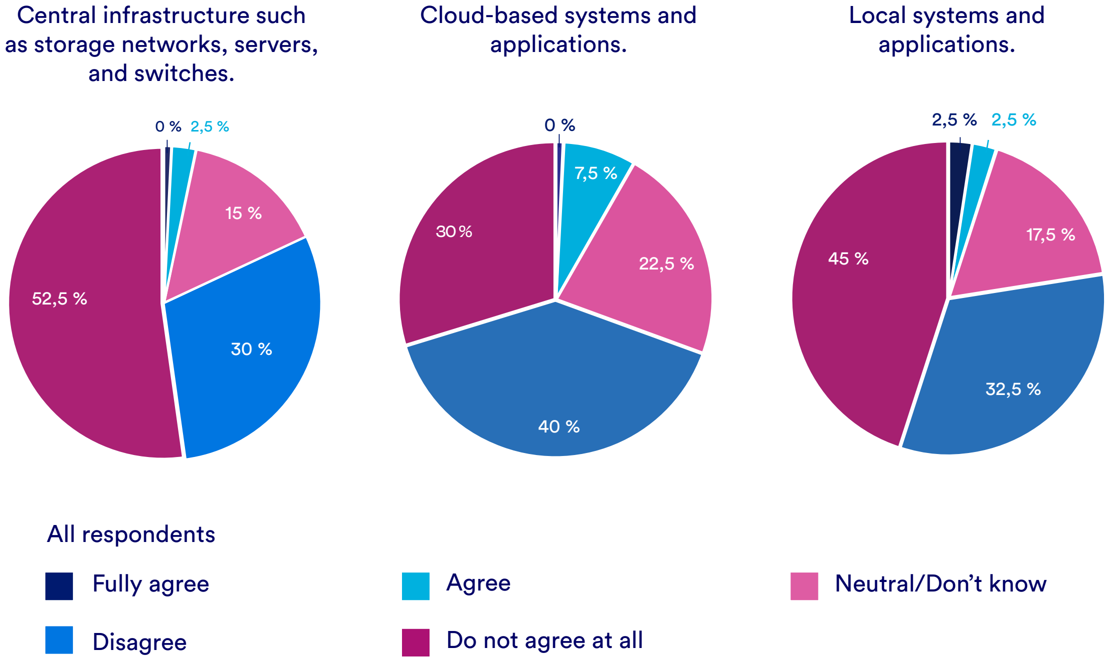
IT leaders in the public sector are less satisfied with their overall IT environment...

Only 5% of public sector IT leaders believe they currently have the best possible IT environment – compared to 16% of their counterparts in the private sector. And while just 2% in the private sector say they are unsure and need to evaluate the question further, the figure is 13% in the public sector.

...but less frequently affected by operational disruptions

Public sector IT leaders are thus more uncertain than those in the private sector about whether their current IT environment is optimal. At the same time, public sector IT leaders report recurring issues with networks, servers, systems, and applications to a lesser extent than those in the private sector.

We often experience issues with



85% continuously replace outdated parts of their IT environment

Outdated systems and servers that no longer receive security updates are a common entry point for hackers. Keeping the IT environment up to date is therefore one of the most important (and cost-effective) measures to prevent data breaches.

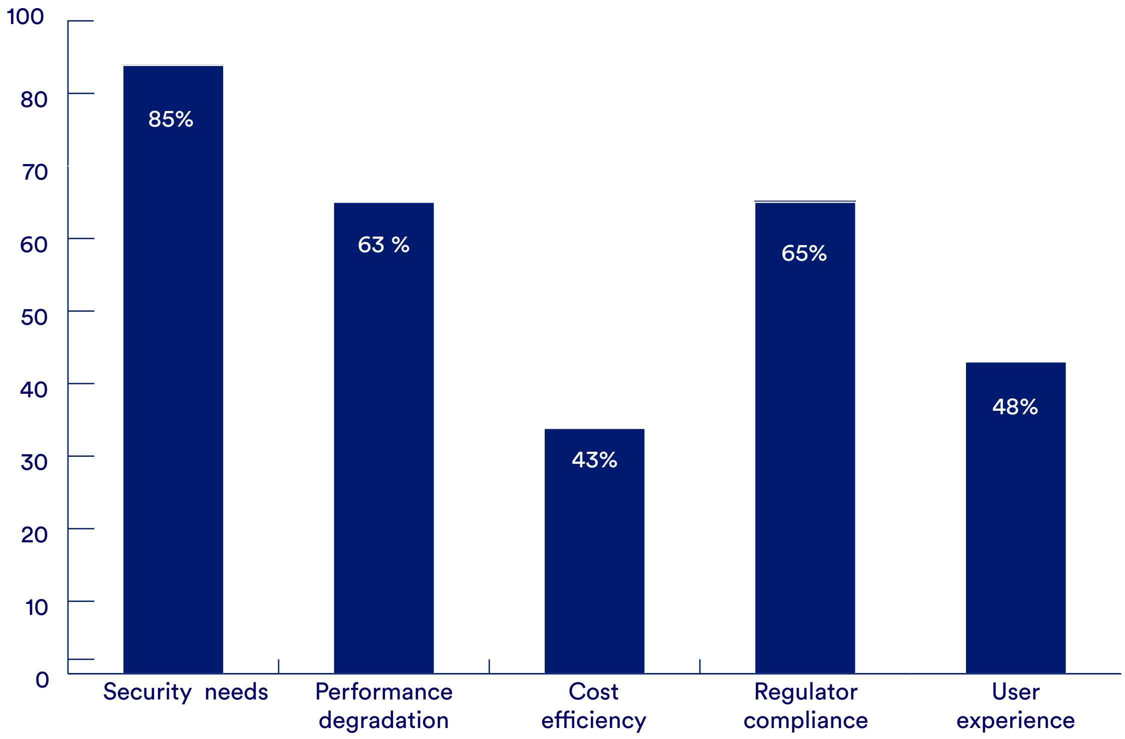
It is therefore encouraging that a large majority of public sector IT leaders (85%) state that they are inclined or highly inclined to replace outdated hardware and expired licenses – even though the share is slightly higher in the private sector (90%).

Security is the primary driver for keeping the IT environment up to date

Security is by far the most important reason for replacing outdated technology in both the private and public sectors. Regulatory compliance plays a greater role for IT leaders in the public sector, while cost efficiency is a more significant driver for those in the private sector.

What are the main reasons for replacing outdated technology?

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



7 out of 10 say that budget impacts the IT department's ability to deliver

Which factors most significantly affect the IT department's ability to deliver in line with organizational goals? For IT leaders in the public sector, budget is the single most important factor. User culture and employees' technical skills also have a major impact, as does access to the right expertise.
Looking at responses from private sector IT leaders, scalability and growth are the only two factors that are valued higher for private than for public sectors.

Which of the following factors affect your/your IT department's ability to deliver in alignment with organizational goals?

(Respondents were allowed to select more than one answer)

Budget:
70%

Expertise:
58%

User culture and the technical proficiency of employees:
65%

1 in 4 store data in the cloud...

Data storage and management are foundational components of any organization's IT infrastructure. According to the survey, the most common setup is a combination of different storage types, such as data centers, cloud storage, and on-premise servers.

One in four IT leaders in the public sector state that they primarily store data in the cloud. This is a higher proportion than in the private sector, where there also appears to be a slightly greater reliance on on-premise servers compared to public organizations.

How do you store data today?

	All	Private	Public sector
1. The 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%

...and have completed a full cloud migration

Today, the cloud is used for much more than just data storage. Cloud migration has been one of the biggest IT trends in recent years. Many organizations have adopted a clear strategy to move more parts of their operations from local infrastructure and hosting to various forms of cloud services. This is reflected in the survey, where only a small percentage report that they have not started, or do not plan to carry out a cloud migration.

The cloud trend appears to have gained more traction in the public sector than in private companies. Nearly one in four IT leaders in the public sector state that their organization has completed a full cloud migration; in the private sector, the corresponding figure is 13%.

How far along are you in your cloud migration journey?

	All	Private	Public sector
1. Full migration	17%	13%	23%
2. Significant migration	37%	38%	38%
3. Partial migration	39%	40%	38%
4. Migration not started	3%	4%	0%
5. No plans to migrate	4%	5%	3%

Expert commentary

“Municipalities and other public organizations often operate with predefined annual budgets. In that context, predictable costs are a clear advantage – such as when purchasing cloud storage as a service.

As an IT leader you need to consider that the more data your organization stores in the cloud, the more important it becomes to have secure and stable connections to it. Today, for example, there are services that allow access to most common cloud platforms via a private connection, without going through the public internet.”

Uffe Traberg, Chief Commercial Officer at GlobalConnect

28% plan to increase their IT outsourcing

When the IT leaders surveyed look ahead, how do they view the balance between managing their network solutions in-house versus purchasing them as services from external partners? Among IT leaders in the public sector, 28% state that they plan to increase outsourcing going forward – compared to 18% in the private sector. The private sector shows a more cautious trend, with a higher share responding “don’t know” compared to the public sector.

What are your future plans – will there be more or less outsourcing of network solutions, such as local area networks?

	All	Private	Public sector
1. More outsourcing	19%	18%	28%
2. No change	62%	60%	58%
3. Less outsourcing	14%	15%	15%
4. Don’t know	5%	7%	0%

Expert commentary

“Interest in outsourcing through managed IT services has definitely increased in recent years. Companies and organizations are facing increasingly complex needs, with more connected devices and rapidly evolving cyber threats. The global shortage of IT talent makes it difficult to manage all of this internally. By partnering with trusted providers who focus on these issues full-time, organizations can leverage the latest technology and expertise – while staying focused on their own core business.”

Emma Helton, Security Product Manager at GlobalConnect

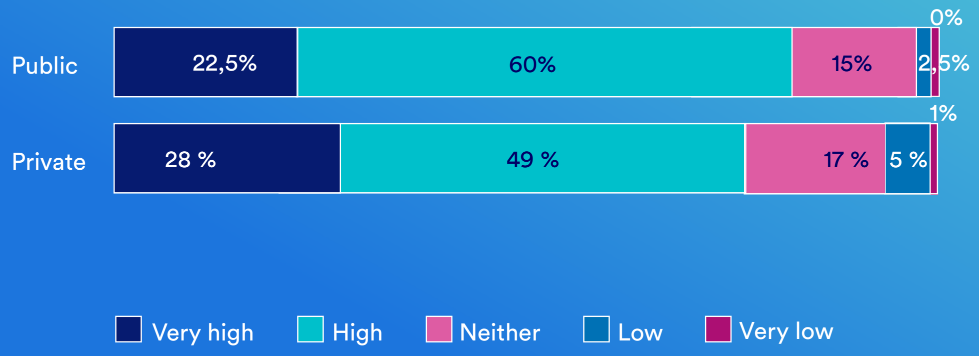
Part 2:

Cybersecurity

8 out of 10 consider their security level to be high

83% of IT leaders in the public sector rate the security level in their organizations as high or very high – a slightly higher proportion than in the private sector (77%).

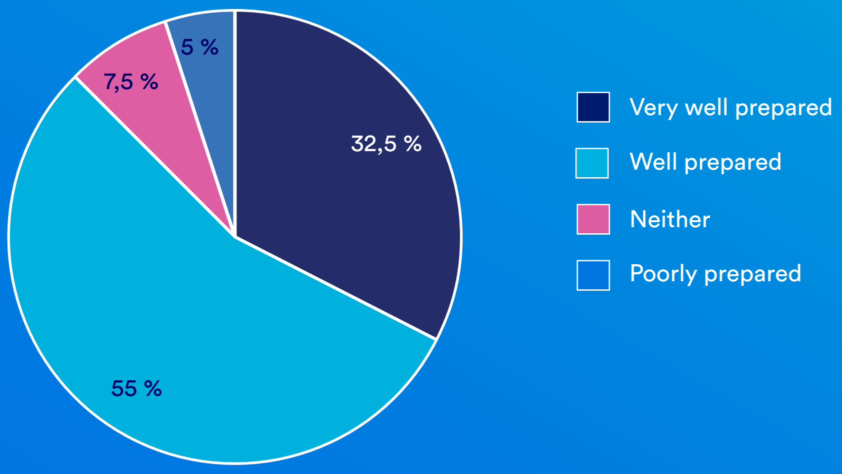
How would you rate your current security level?



Nearly 9 out of 10 say they can recover lost data

The ability to restore lost data after a cyberattack or IT failure is a critical cornerstone of modern cybersecurity. In this area as well, the public sectors IT leaders express slightly more confidence than their counterparts in the private sector.

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



Expert commentary

"It would be fantastic if the security levels were truly as high as IT leaders report. Unfortunately, it's more likely that risks are underestimated and preparedness overestimated. Even if you have the capability to recover lost data, there's often no room in the budget for the costs involved. A 2024 report, for example, shows that 43% of the data affected by a ransomware attack cannot be recovered – it's lost for good."

Øystein Snekkerlien, Security Strategist at GlobalConnect

Just over half are concerned about IT attacks or failures

53% of public sector IT leaders express concern about being affected by an IT attack or system failure. The corresponding figure in the private sector is higher: nearly 7 out of 10.

53% of public sector IT leaders fear IT threats.

1 in 3 report that their organization has been attacked recently

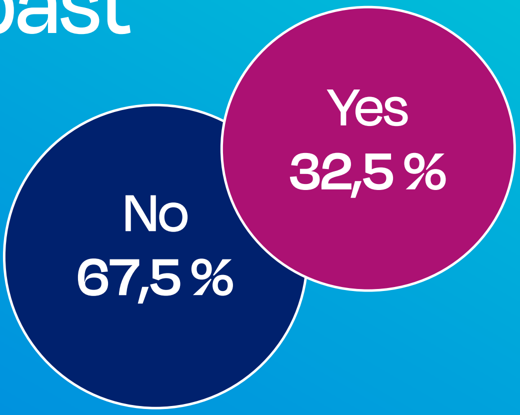
One in three public sector IT leaders state that their organization has been subjected to an IT attack within the past two years. A clear trend in the private sector is that attacks are more common among larger companies. Among those with the highest revenue, more than half of the respondents report that their company has been targeted.

Expert commentary

"Public sector organizations have become aware that they, too, are targets for cyberattacks, while struggling to compete with the private sector for top cybersecurity talent. In recent years, we have particularly seen an increase in a type of attack that less frequently targets private companies. Instead of financial motives, as with ransomware attacks, these actors aim to destabilize our societies, spread fear among citizens, and undermine trust in our institutions. As a result, IT systems connected to public services – such as water supply – are being targeted."

Uffe Traberg, Chief Commercial Officer at GlobalConnect

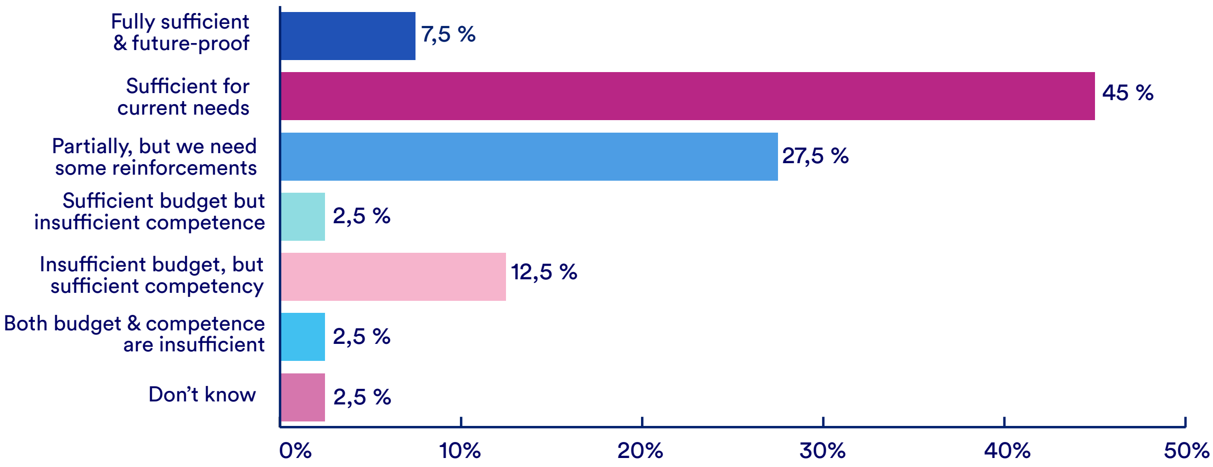
Have you been subjected to an IT attack in the past two years?



45% need reinforcement to meet desired security levels

Lack of budget and internal expertise (or both) prevents nearly half of the IT managers in the public sector from maintaining the level of security they believe their organization should have. Only 8% say they have sufficient resources to meet both current needs and future-proofing requirements.

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



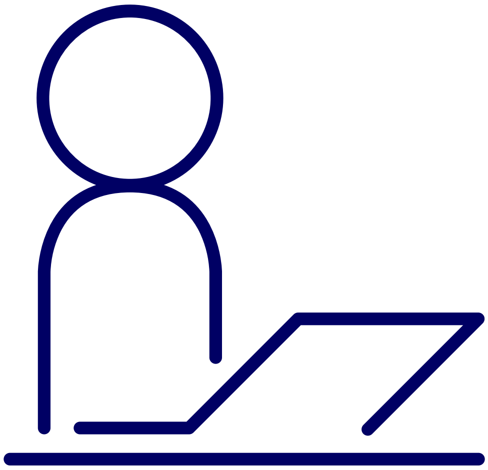
Expert commentary

“It has been difficult for IT leaders to gain support for investments in cybersecurity. Too many organizations have assumed that attacks happen to others, not to us. But recently, cybersecurity has climbed higher on the agenda. This shift is partly driven by geopolitical tensions, but even more so by stricter regulations such as NIS2. At the same time, the survey reveals a lag, where IT leaders still lack the resources needed to future-proof their operations.”

Øystein Snekkerlien, Security Strategist at GlobalConnect

1 in 5 in the public sector rate cybersecurity awareness as worryingly low

The human factor appears to be a vulnerability worth focusing more on in the future. IT leaders' trust in employees is significantly lower than their confidence in the overall security level.
A full 20% of public sector IT leaders rate employees' cybersecurity knowledge as low or very low – compared to 12% in the private sector.



Expert commentary

"Cybersecurity knowledge needs to extend beyond the IT department so that all employees understand how they can help reduce risks. But just as important is building your IT infrastructure in a way that makes it easy to do the right thing. If it's too complicated, employees will find ways to bypass your security restrictions."

Øystein Snekkerlien, Security Strategist at GlobalConnect

Part 3:

The Future

Fewer than 50 % are prepared for future technological developments

The rapid advancement of technologies, especially AI, brings new demands for handling large volumes of data efficiently. Are today's IT departments ready to scale their infrastructure to harness the benefits of emerging innovations?

Among IT managers in the public sector, 45% consider themselves well or very well prepared; compared to 55% in the private sector

How prepared is your organization for future developments (e.g., the data volumes required by AI)?

	All	Private	Public
1. Very well prepared	9%	11%	10%
2. Well prepared	41%	44%	35%
3. Neither	35%	32%	40%
4. Poorly prepared	12%	12%	13%
5. Very poorly prepared	2%	2%	3%

Expert commentary:

"With the exponential increase in data volumes driven by AI, it is crucial for organizations to invest in robust data infrastructures. Cloud services and edge computing are becoming increasingly central to efficiently manage and process large amounts of data. As an IT leader, you also need to build a flexible and scalable infrastructure that can adapt to future technological shifts. And last but not least: invest in training and skills development to ensure that your employees are ready to work with AI technologies."

Emma Helton, Security Product Manager at GlobalConnect

35% don't know whether they are covered by the NIS2 directive

The NIS2 directive means that a range of companies and public sector organizations must comply with stricter cybersecurity requirements. The survey shows that it is far from clear who is actually subject to the regulation: more than one in three public sector IT leaders say they don not know whether their organization is covered or not. Among IT managers in the public sector, 45% consider themselves well or very well prepared; compared to 55% in the private sector

Is your organization subject to the NIS2 directive?

	All	Private	Public
1. Yes	34%	36%	28%
2. No	40%	38%	38%
3. Don't know	26%	26%	35%

What is the NIS2 directive?

The EU's NIS2[2] directive was adopted in October 2024 and will be incorporated into the national legislation of each member state. Its overarching goal is to strengthen cyber resilience across the entire Union. Organizations covered by the directive must meet strict requirements for cybersecurity and incident reporting. Non-compliance may result in substantial fines.

European Parliament & Council of the European Union. (2022, December 14).
https://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=CELEX:32022L2555&from=EN

Expert commentary:

“The fact that so many IT leaders in the survey don’t know whether they are covered by NIS2 is concerning. Since the directive also affects subcontractors across multiple tiers, it’s almost safe to assume that your organization will need to comply. My impression is that directives like NIS2 and DORA, have served as a much-needed wake-up call, forcing companies and organizations to raise the bar when it comes to cybersecurity.”

Søren Gjevert Petersen, Head of Security Services at GlobalConnect

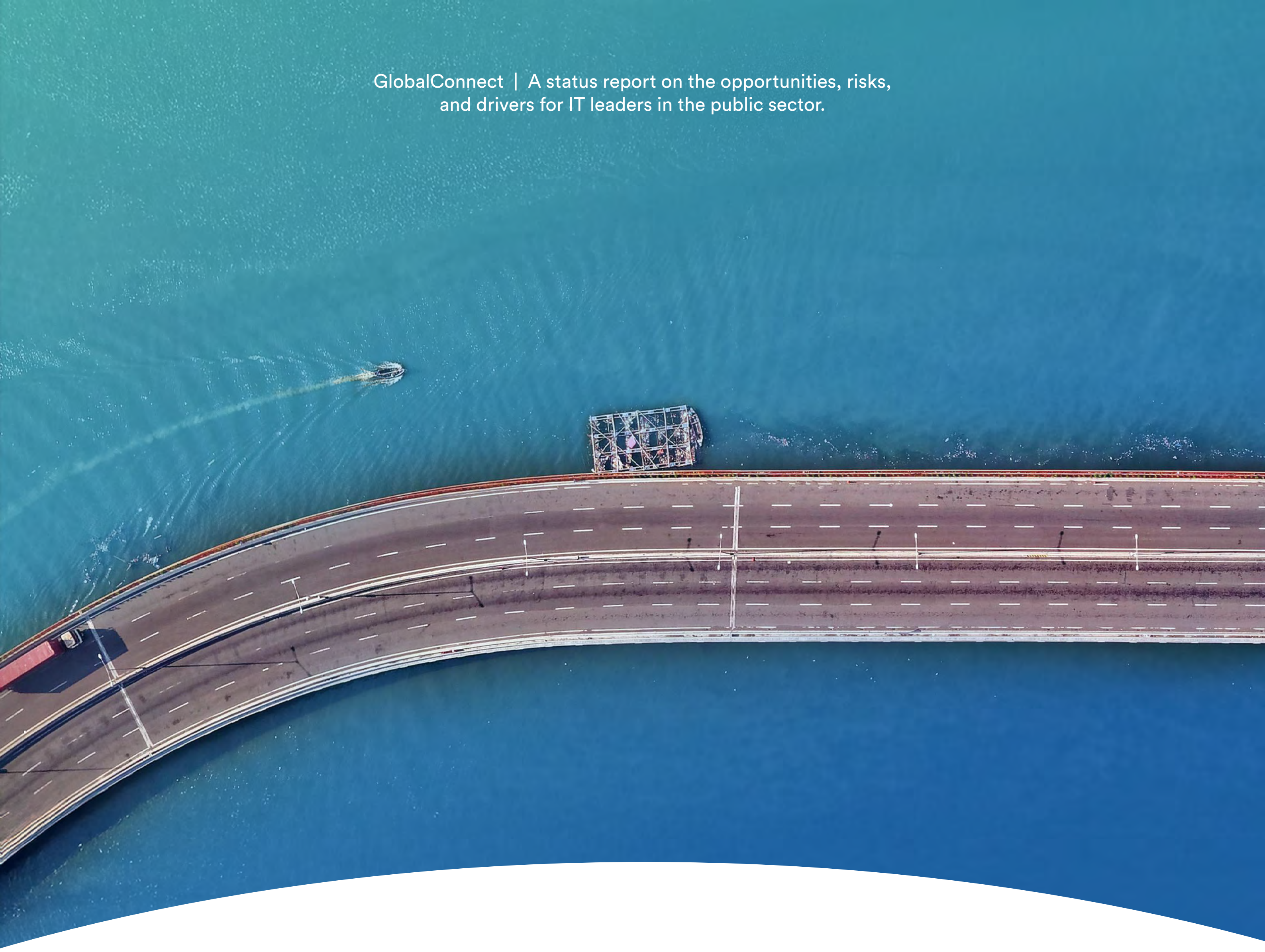
4 out of 10 need more resources to ensure regulatory compliance

The scale of the adjustments required to meet the demands of NIS2 and other directives and regulations depends on the organization's current state. But there appears to be a widespread need for reinforcement: 40% of public sector IT leaders say they lack sufficient budget, expertise, or both to achieve compliance. One in four are unsure and need a more thorough evaluation.

Do you have sufficient budget and expertise to ensure regulatory compliance, such as the NIS2 directive?

	All	Private	Public
1. Fully sufficient budget and future-proof	11%	13%	8%
2. Sufficient for current needs	31%	32%	20%
3. Partially, but we need some reinforcements	25%	25%	23%
4. Insufficient budget but sufficient expertise	4%	4%	8%
5. Sufficient budget but Insufficient expertise	4%	5%	3%
6. Both budget and expertise are unsufficient	6%	5%	8%
7. Unsure, need deeper evaluation	13%	10%	25%
8. Other, please specify	5%	6%	8%

> "You can not just buy a top-tier solution and think you are done."
>
> Søren Gjevert Petersen, Head of Security Services at GlobalConnect



Expert commentary:

“The directive emphasizes that security must be an integrated part of the IT infrastructure, not something you add afterward. Much of it comes down to the fundamentals, such as lifecycle management and classifying your assets so that each component receives the appropriate level of protection. If you are already used to working with the original NIS directive and certifications like ISO 27000, you will have a head start when it comes to NIS2. Among other IT leaders, we see greater uncertainty. But regardless of where you are starting from, it is wise to take a long-term view and break the transition into manageable phases to make the most of your resources.

By all means, bring in external partners, but remember that responsibility can not be outsourced. That is why it is essential for IT leaders to familiarize themselves with the legislation alongside legal experts and take ownership of both implementation and ongoing compliance. This is not a one-time investment. You can not just buy a top-tier solution and think you are done.”

Søren Gjevert Petersen, Head of Security Services at GlobalConnect

1 in 4 have a good understanding of the risks and opportunities of quantum technology

One topic that's getting less attention than AI and NIS2 right now, but is likely to have major consequences in the future is the development of quantum computing. The quantum issue, and the looming "Q Day," does not appear to be a high priority among the survey participants.

Half of public sector IT leaders report having poor or very poor knowledge of the opportunities and risks associated with quantum technology, while one in four say they have good or very good understanding.

How well do you understand quantum technology and its opportunities/security risks?

	All	Private	Public
1. Very good	3%	2%	10%
2. Good	18%	20%	15%
3. Neither good or bad	30%	30%	25%
4. Poor	31%	33%	25%
5. Very poor	18%	15%	25%

What is a quantum computer?

A quantum computer uses the principles of quantum mechanics to perform calculations. Unlike classical computers, which operate with bits (0 or 1), quantum computers use so-called quantum bits, or “qubits,” which can exist in multiple states at once. This means that certain types of problems, especially within cryptography, simulation, and optimization – can be solved significantly faster than with traditional computers. This brings both opportunities and risks.

What is Q Day?

Many of today’s solutions for secure and private communication rely on encryption keys being so complex that a traditional computer cannot decode the information within a reasonable time. However, in the not-so-distant future, quantum computers are expected to reach the computational power required to quickly and easily break these codes. This point in time is referred to as Q Day, and it marks the moment when commonly used encryption methods such as RSA encryption, can no longer be considered secure.

Expert commentary:

“Q Day is a bit like when the millennium shift was closing in, only without a known date. The window of time is shrinking, but there’s still an opportunity to act. The most important thing you can do as an IT leader right now is to get a clear overview of your IT environment and your data, making sure everything is well-structured and properly classified. That way, the day you need to migrate critical parts to quantum-secure solutions, which are currently being developed, the process will be much faster and more manageable.”

Martin Højriis Kristensen, Director of Customer Technology at GlobalConnect

Conclusion
The balancing act behind smarter IT in the public sector

Being an IT leader today is no small task. The more unpredictable the world becomes, the more critical it is to have a solid strategy for areas like data storage and network security. At the same time, rapid technological change and growing cyber threats demand flexibility and fast responses.

This balancing act is especially tough in the public sector. Here, IT investments are tied to strict procurement processes and long contract periods. Meanwhile, leaders face pressure to stretch limited resources and deliver reliable, secure services.

So how do you keep your IT environment up to date between procurement cycles? And how do you attract and retain the right talent during a global shortage of IT professionals?

Our survey shows that many public sector IT leaders see outsourcing - such as cloud services and managed network operations - as a way forward. The benefits are clear. It shows reduced internal workload, more predictable costs, and less reliance on individual employees.

But with more outsourcing comes greater responsibility. As a buyer, you still need to ensure that systems work together, meet compliance requirements, and support your overall IT strategy. That is why choosing the right partners is essential - not just for individual services, but for integrated, long-term solutions and support.

About GlobalConnect

GlobalConnect is one of the leading digital infrastructure and data communication providers in the Nordic region, driving more than half of all data traffic in and out of the Nordics. GlobalConnect delivers fiber-based broadband services to more than 830,000 private consumers and end-to-end connectivity solutions to 30,000 B2B customers via its 244,000 kilometer fiber network across Denmark, Norway, Sweden, Germany and Finland. It's our way of keeping society running and enabling the innovations of tomorrow.

GlobalConnect