nixu cybersecurity.

CYBERSECURITY INDEX

Report 2023

Table of contents

“

81% of organizations view business resilience as the foremost reason for their cybersecurity investments.

Introduction

In our continued commitment to understanding the evolving landscape of cybersecurity, we present the Nixu Cybersecurity Index 2023. We have, once again, delved deep into the insights of business, IT, and security leaders across Europe, particularly focusing on the Nordics and northern Europe. Through our comprehensive assessment, we've gauged the cybersecurity maturity of over 370 organizations, encompassing various facets of cybersecurity operations, from their current status and management to investments and anticipated advancements.

Last year, Nixu unveiled its first Cybersecurity Index report, establishing a foundation for what we envisioned as an annual endeavor. Our core objective remains consistent: to discern the maturity levels of organizations in managing cybersecurity and to identify the distinct practices of the more advanced entities. The study is based on a combination of an extensive survey and interviews.

While we have retained core parameters from the previous year, for the 2023 Index, we have also introduced a few new elements to enrich our analysis. For instance, new questions were added to explore the primary drivers of cybersecurity investments and to look into emerging topics like AI, which has surged with a force on everyone's radar since last year. We also asked about operational technology, OT, which is necessary for a wide range of companies that use control systems for automation and machinery, for instance, in manufacturing, energy and utilities, and building management..

What's equally noteworthy, in 2023 we managed to expand our survey to include more companies and respondents from different roles and types of industries, as well as wider geographical scope. Although this means that a direct comparison with last year's report might not be seamless, the enhanced data quality, courtesy of a doubled sample size, offers more compelling insights, and the broader respondent base provides us with a more nuanced geographical comparison across countries.

We trust that you'll find this report insightful and hope it serves as a valuable resource, enabling you to tailor strategies for your organization.

Key findings

1 Business resilience drives investments in four out of five organizations

Over recent years, many organizations have experienced disruptions due to significant global events, affecting their operations and business continuity. This context underscores why 81% of organizations view business resilience as the foremost reason for their cybersecurity investments.

Resilience has consistently been a top priority, both in the past year and for the upcoming 12 months. Notably, the energy and utilities sector places the highest importance on business resilience, with 93% of respondents stating it as their first choice.

2 AI is everywhere – unprecedented security concerns emerge

Suddenly, artificial intelligence has surfaced as a prominent topic in cybersecurity. This surge likely stems from the buzz surrounding generative AI and the challenges in foreseeing its ramifications, especially its growing role in business solutions.

While AI has long been a staple in cybersecurity, notably in detection tools to enhance efficiency, emerging AI-driven techniques amplify the potential for malicious players. These actors can refine their tactics in social engineering, phishing, ransomware, and deepfake content, and even deploy AI in Denial of Service (DoS) attacks. Conversely, from a defense perspective, AI bolsters advanced technology and boosts productivity.

3 Top priorities: Security monitoring, awareness, and IAM

Enhancing security monitoring, raising security awareness, and refining identity and access management (IAM) stand out as primary development objectives, with approximately 40% of respondents highlighting their significance. This sentiment is mirrored in the expectations organizations have towards cybersecurity service providers. Early threat detection is the most valued service, chosen by 82% of respondents.

Interestingly, last year’s prime focus, supply chain management, appears to have declined in priority. Yet, supply chain security remains crucial in meeting compliance mandates, particularly concerning the Network and Information Security Directive (NIS2) and the Digital Operational Resilience Act (DORA), which are now of elevated importance.

4 Dramatic performance gap between the best and the rest

Organizations with a Cybersecurity Index of 75 or higher distinctly outperform their counterparts. What sets them apart?

A notable 58% of these top performers prioritize risk management as a vital capability, in contrast to 33% of the lower-performing organizations. A significant 76% include cybersecurity in their executive management discussions, compared to just 18% of the remainder. These leading organizations allocate a more substantial portion of their total budget to cybersecurity. They invest more in cybersecurity, not primarily for cost efficiency but for robustness. Additionally, their information security teams are more expansive.

5 Increasing internal headcount will be tough

Organizations show modest intentions to expand their internal cybersecurity teams over the next three years. Alarmingly, 59% already face challenges in hiring the necessary cybersecurity expertise. Considering only the demand from respondents, the total requirement for specialists stands at approximately 1,300.

In practice, this means that the trend towards outsourcing cybersecurity will likely intensify. A mere 7% of organizations view in-house teams as the answer to maintaining cybersecurity proficiency.

> **“**
>
> **Top performers prioritize risk management as a vital capability.**

Trending topics in cybersecurity

AI became the #1 cybersecurity topic in 2023, while concerns about regulations are rising

CYBERSECURITY TOPICS THAT HAVE INCREASED IN IMPORTANCE, **RECENT 12 MONTHS**

- AI
- Compliance
- Cloud security
- Phishing
- Business resilience
- Supply chain security
- Ransomware

CYBERSECURITY TOPICS INCREASING IN IMPORTANCE, **NEXT 12 MONTHS**

- Regulations and their implementation **(NIS2, EUCS, DORA*)**
- AI
- Cloud security
- Phishing
- Business resilience

CYBERSECURITY TOPICS THAT WERE MOST IMPORTANT **IN 2022**

- Ransomware
- Phishing
- Operational technology security
- Vulnerability management
- Supply Chain Attacks

WHAT RESPONDENTS SAY

"AI in security solutions, public cloud security/posture management."

"Compliance with industry best practices and various customer-mandated security requirements."

"Compliance as NIS2 is closing in."

"AI, AI, AI, AI."

"DORA and compliance requirements will be the main focus."

"Cyber defense and Russia's aggression are the main things right now."

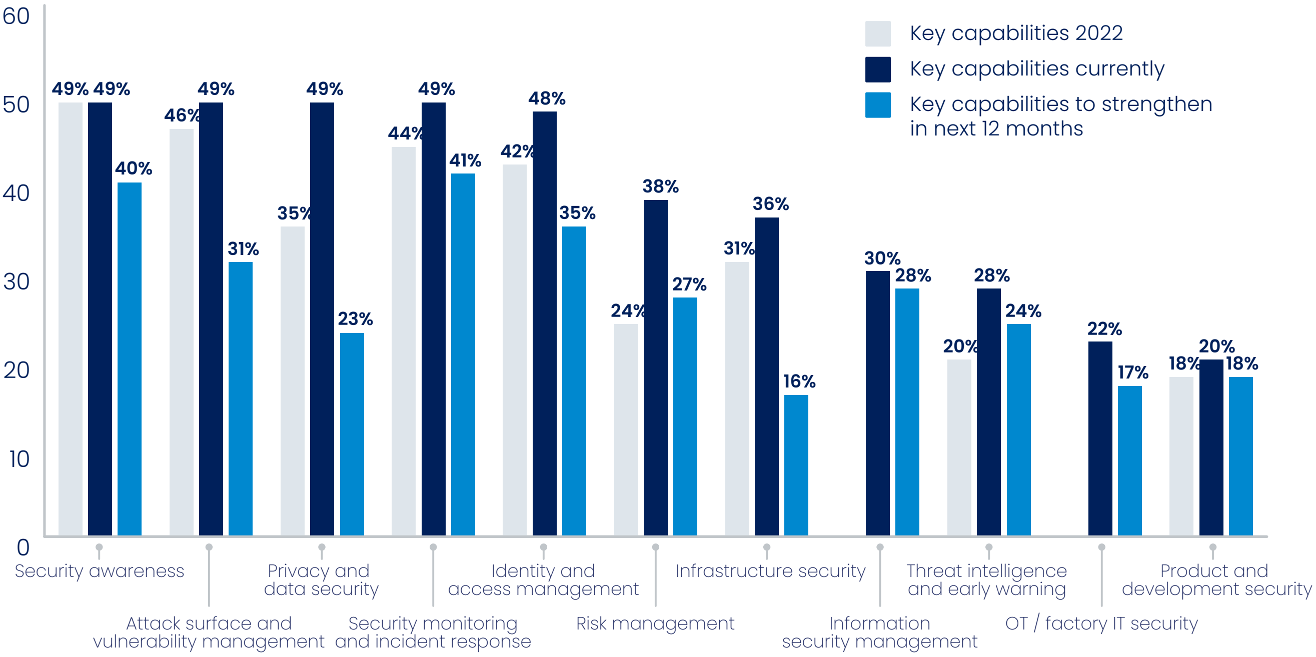
"Phishing attacks, targeted phishing, challenges related to remote work and zero trust."

* NIS2 = Network and Information Security Directive (EU-wide legislation on cybersecurity)
EUCS = European Cybersecurity Certification Scheme for Cloud Service
DORA = Digital Operational Resilience Act (affects the financial sector only)

Key capabilities in cybersecurity

Currently, capabilities in four different areas are perceived as equally critical. Among these, security monitoring and incident response, as well as security awareness stand out as critical capabilities that organizations intend to strengthen the most in the upcoming months.

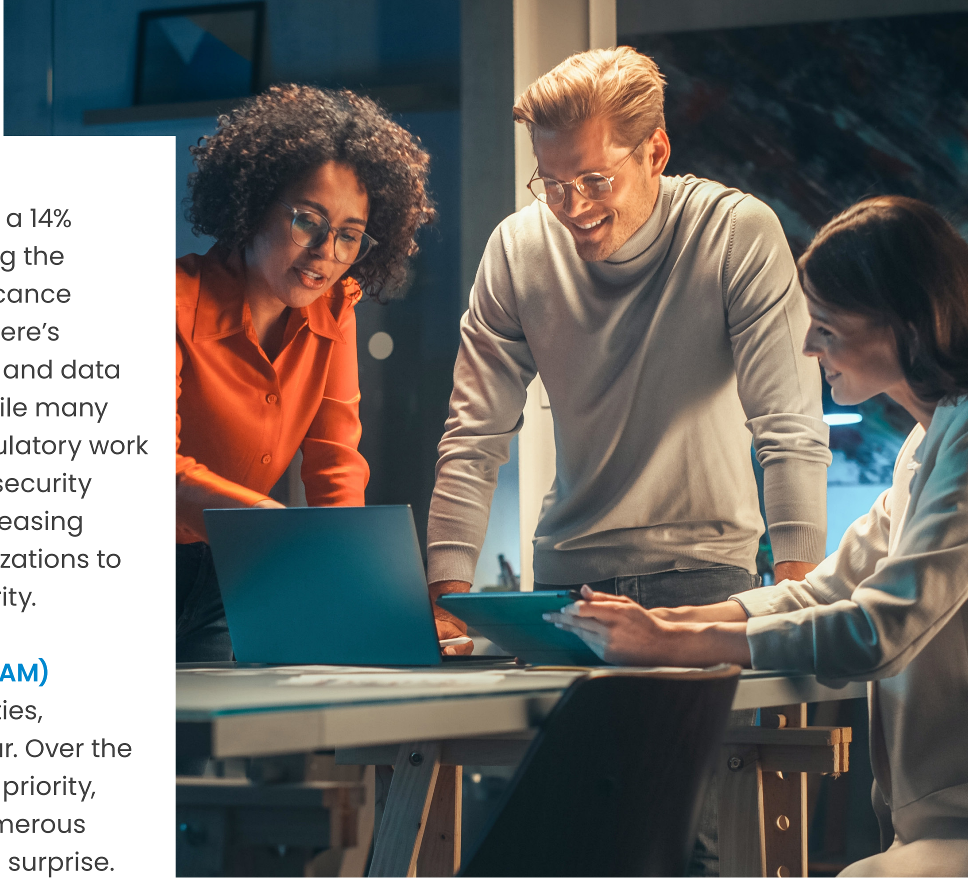
Assessment of most critical capabilities currently and development plans for the next 12 months. Select 3–5 most critical areas.



Security monitoring and incident response is clearly seen as a top capability both presently and for the foreseeable future. Notably, its significance has risen from 44% to 49% since last year, underscoring organizations' emphasis on sustaining business resilience amidst the evolving cybersecurity threat environment. Leveraging advanced, AI-driven monitoring, organizations are better positioned to detect early signs of attacks. Coupled with refined response mechanisms, they can mitigate the repercussions of any incident.

Security awareness remains consistent with 2022 levels, marking it a vital capability that organizations are keen to enhance. Efforts to increase employee comprehension of cybersecurity persist, especially within the health and social care sector.

Attack surface and vulnerability management is currently deemed a key capability, particularly in the public sector and defense organizations. However, respondents anticipate its importance will wane over the next year.



Privacy and data security witnessed a 14% surge from last year, ranking it among the top four capabilities. Its future significance is projected to decline sharply, but there's room for interpretation since privacy and data security are somewhat separate. While many organizations may soon declare regulatory work with privacy done and dusted, data security initiatives remain on the horizon. Increasing regulation is likely to motivate organizations to develop their privacy and data security.

Identity and access management (IAM) trails closely behind the top capabilities, registering a 6% growth from last year. Over the next year, fortifying IAM ranks third in priority, and given its foundational role in numerous critical cybersecurity areas, this is no surprise. IAM demands heightened attention due to regulatory compliance and governance issues. The increasing importance of IAM is also driven by expanding cloud adoption and the growing complexity of IT and OT ecosystems. Additionally, the advent of zero trust security architecture, based on determining who exactly is trying to access and use digital systems, imposes its own requirements on IAM. Ultimately, modern IAM solutions enable zero trust.

In addition, the realm of Customer Identity and Access Management (CIAM) is also evolving, driven by the unique needs of managing customer identities, enhancing user experiences, and ensuring data privacy..

Risk management has seen a notable ascent, from 24% in 2022 to 38% in 2023. The uptick suggests a growing number of organizations recognize the advantages of accurate risk assessment, forming the bedrock for sensible cybersecurity investments. This capability is particularly favored by the energy and utilities sector. Also, Gartner highlights this capability in their Top Eight Cybersecurity Predictions for 2023–2024. They predict that by 2025, while 50% of companies will attempt to address it, more than half will not succeed.

Information security management, a newcomer in this edition of the Cybersecurity Index, is crucial for both compliance and smart investments. Particularly the financial sector respondents emphasize its importance.

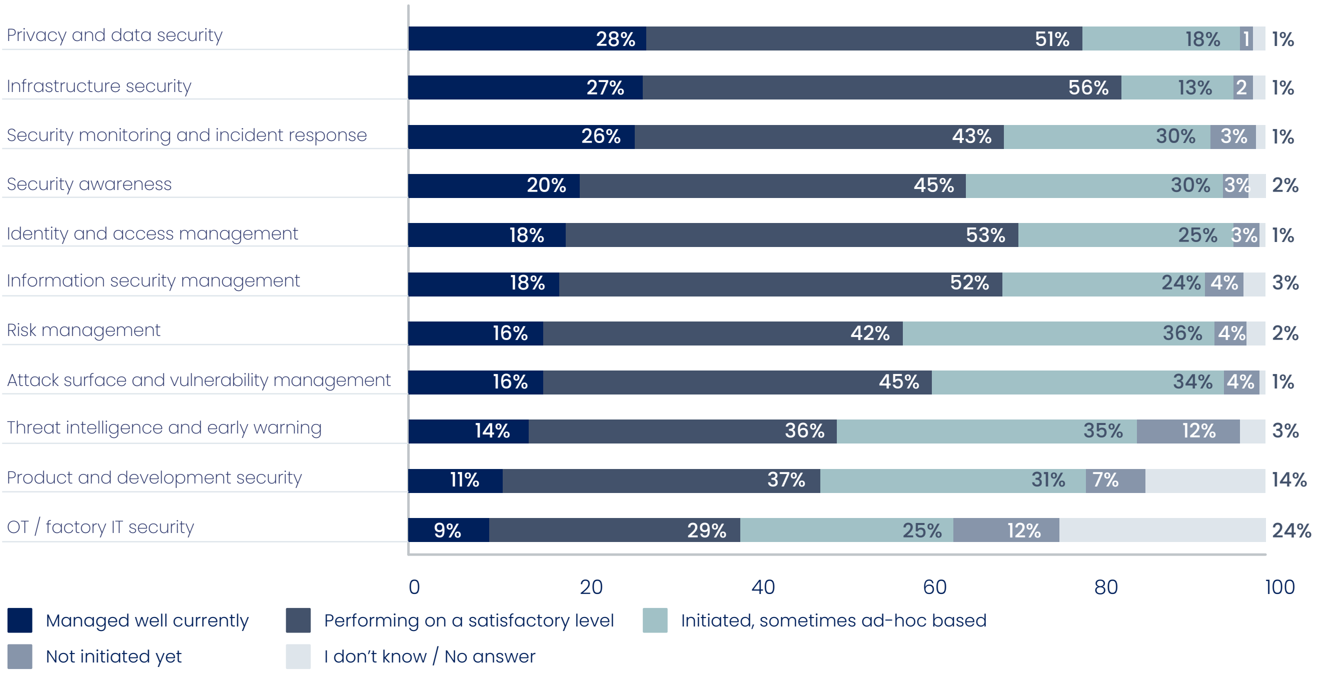
Operational technology (OT) / factory IT security is another debutant in our report. It was noted as a key capability especially by the energy and utilities sector, where it was selected by 64% of the respondents, and the industrial sectors, where it was chosen by 47%. The public and defense sectors, in turn, tend to prioritize **threat intelligence and early warning**.

Country-wise, the selection of critical capabilities varies rather clearly. In **Sweden**, security monitoring, security awareness, and attack surface and vulnerability management take precedence over other Nordic countries, and the same trio topped in 2022. **Finland** now prioritizes privacy and data security, which jumped from fifth position in 2022 right to the top, followed by security monitoring and security awareness. **Norwegian** entities aim to enhance privacy and data security, while **Denmark** emphasizes IAM and risk management, both now and in the future.

The current state of cybersecurity

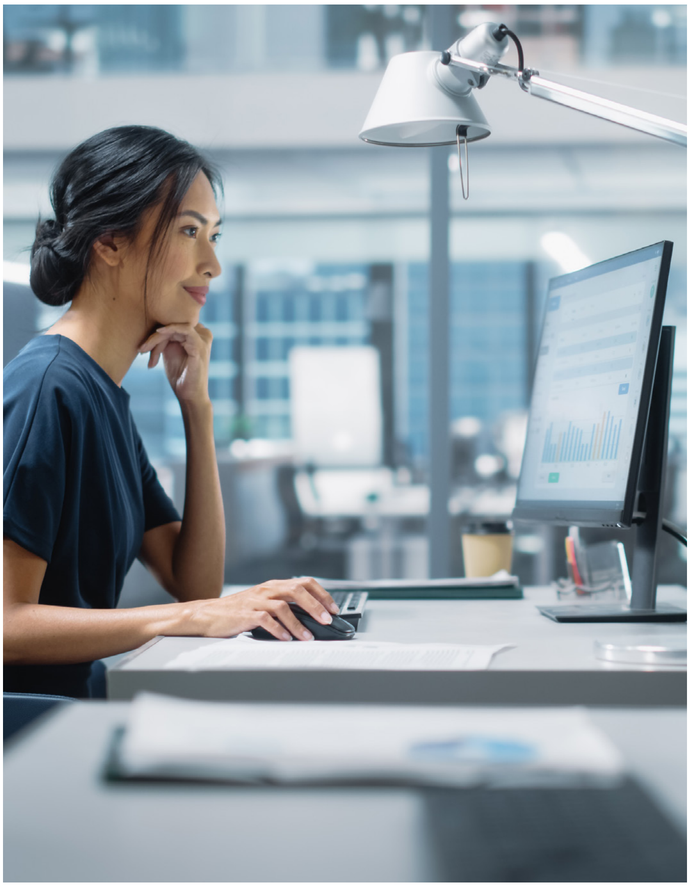
Responses in 2023 claim that privacy and data security, as well as infrastructure security are the best managed cybersecurity capabilities in northern Europe.

How would you describe the current state of the following capabilities of cybersecurity in your organization?



Organizations' self-evaluation of their cybersecurity capabilities in 2023 shows a somewhat inconsistent progression compared to 2022. Six of the nine capabilities assessed in both years have seen improvements, while three have regressed. New capabilities charted this year are information security management and OT/factory IT security.

The concerted efforts of organizations appear to have enhanced the state of **privacy and data security**. A notable 79% of entities consider this domain their most adeptly managed capability. With a marked upswing, privacy and data security now stands out as the top-managed capability when considering only the responses rated as "managed well." The health and social care sectors are most confident in this area. Alongside the finance sector, they underline the significance of cybersecurity more than any other industry, with 94% incorporating cybersecurity discussions at the executive management level.



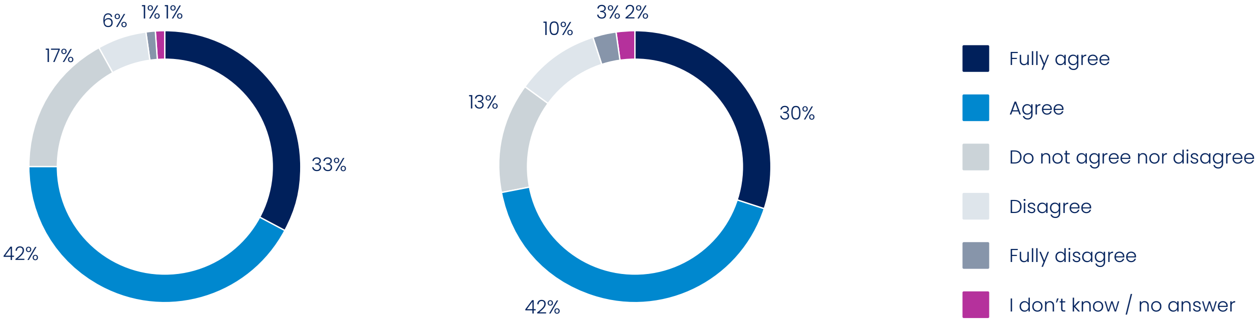
While **infrastructure security** capabilities remain robust, there's a slip with only 27% assessing that it's "well managed" compared to 33% last year. However, a commendable 80% believe their infrastructure security is at least at a satisfactory standard. Based on self-assessment, health and social care also excel at this capability.

Yet, there is a looming concern that organizations might harbor misconceptions about their cybersecurity stature. Investing heavily in specific areas can skew perceptions, potentially leading to overconfidence and misplaced assurance.

Ranked last is **OT / factory IT security**, which had the highest proportion of non-responses. Often, IT security personnel within organizations lack visibility into the management of OT.

75% of companies say that cybersecurity is on the executive management team's agenda

Attention to cybersecurity issues seems to be waning at the executive board level when compared to 2022. The heightened alertness to cyber threats, initially triggered by Russia's invasion of Ukraine, might have diminished, coupled with increasing financial concerns within organizations. There are differencies between industries. In the finance and IT sectors, 85% address cybersecurity at the board level, while for others, the average is just 50%.



Cybersecurity is on our executive management team's agenda

Cybersecurity topics are reported on the board level in our organization

Charts include respondents from all the industries

Based on self-assessment, Finland seems to lag behind other Nordic countries in the development of many of the assessed cybersecurity capabilities

Percentage of respondents who feel the capability is managed well.

	Finland	Sweden	Denmark	Norway
Privacy and data security	24%	32%	28%	39%
Security monitoring and incident response	23%	30%	24%	26%
Infrastructure security	23%	30%	28%	39%
Security awareness	18%	16%	28%	32%
Identity and access management	18%	14%	21%	23%
Information security management	16%	19%	10%	23%
Attack surface and vulnerability management	12%	14%	24%	19%
Risk management	11%	19%	28%	16%
Threat intelligence and early warning	10%	16%	17%	19%
Product and development security	8%	14%	10%	23%
OT / factory IT security	6%	5%	17%	26%
Average	15%	19%	21%	26%

□ 0-9% ▤ 10–19% ▦ 20–29% ■ 30% or more

Norwegian organizations stand out compared to other countries, with 26% deeming their cybersecurity well-managed. However, it's worth noting that the average size of the responding organizations from Norway was smaller, and the industry representation was limited.

In contrast, Finnish organizations exhibit less confidence in nearly all capabilities. Finland has now overtaken Sweden, which trailed in 2022 in terms of overall cybersecurity maturity. This shift invites speculation – it doesn't necessarily signal a tangible change.

One possible explanation is that the Finnish respondents comprised a higher percentage of business decision-makers, who might lack a precise understanding of their cybersecurity status. Additionally, Finland's economy leans heavily on the industrial sector, where privacy concerns aren't as paramount as in consumer-oriented businesses or services. The recent NATO membership and a potentially declining economy might also influence the self-assessments in Finland.

"Norwegian organizations stand out when compared to other countries, with 26% deeming their cybersecurity well-managed."

Cyber threats harming own operations is the primary concern

Respondents are concerned about the realization of cybersecurity risks. The most frequently cited issues are related to operational challenges within organizations, potential harm to reputation, skill and competency deficits, implications for their customers' businesses, and data breaches.

68% are concerned by the potential harm cyber threats may cause their operations.

44% worry that cybersecurity issues may damage the corporate image.

39% find the lack of expertise to manage cybersecurity concerning.

38% worry that a customer's business may be harmed.

34% point out that intruders can access their business data.

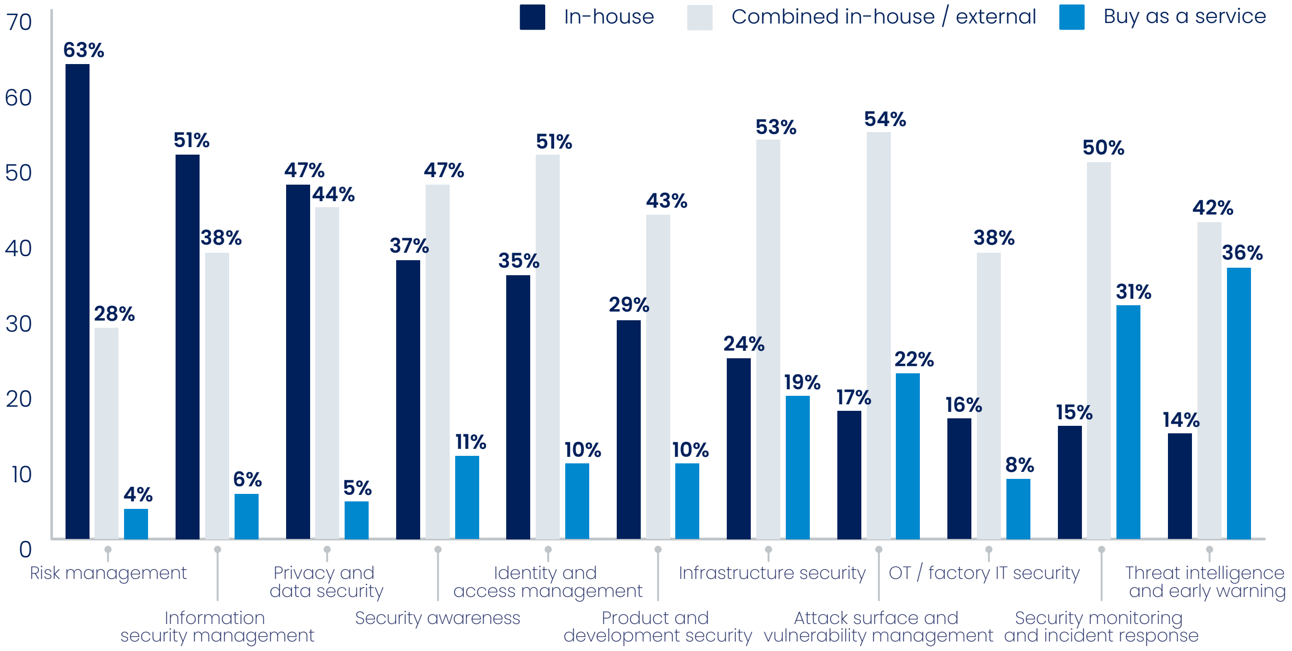
31% are afraid their supply chain or vendors are not able to secure their own systems.

> The primary reasons for outsourcing cybersecurity include a shortage of professionals, high competency demands, limited internal resources, and the expense of maintaining them.

Managing competences

Organizations are most likely to buy threat intelligence and security monitoring as a service – Risk management is the most common in-house capability

Which capabilities does your organization plan to have in-house and which to outsource?



Achieving an adequate scale in **threat intelligence and early warning** internally is challenging. This explains why it's the most sought-after cybersecurity service. Similarly, the expertise needed for **security monitoring and incident response** is so advanced that few organizations can manage it in-house. This duo also topped the preferences for outsourcing in 2022.

Generally, organizations prefer a blend of internal and external capabilities. **Attack surface and vulnerability management**, along with **infrastructure security**, are commonly managed in collaboration with a cybersecurity service provider. The exact division of responsibilities between internal and external teams was not examined, but we know it tends to vary widely based on the capability and the organization.

There continues to be a pronounced tendency to keep **risk management** as well as **privacy and data security** as in-house competencies. This approach seems risky for several reasons. More than one in three organizations acknowledge their risk management is in its infancy, and only 16% believe they manage this area effectively.

The primary reasons for outsourcing cybersecurity include a shortage of professionals, high competency demands, limited internal resources, and the expense of maintaining them. Factors favoring an in-house approach include regulatory considerations, understanding the business, a preference for internal strategic competencies, the high cost of services, and, occasionally, national security considerations.

What respondents say about the difficulty and cost of recruiting sufficient in-house expertise – outsourcing is favored

KEY REASONS FOR **IN-HOUSE COMPETENCES**

"In-house people ensure business alignment and alignment with cyber risk appetite."

KEY REASONS FOR **COMBINED APPROACH**

"It is difficult to recruit people with sufficient expertise as the market for these people is pretty slim and, therefore, also very competitive. Moreover, topics like security awareness are best executed with hybrid solutions. The best solutions and experts are usually commercially available and not needed around the year."

"Security is key for the trust in our products and brand, leading to a large portion in-house. However, we need to buy best-of-breed threat intel and cyber defense monitoring for fast detection of advanced threats."

KEY REASONS FOR **OUTSOURCING**

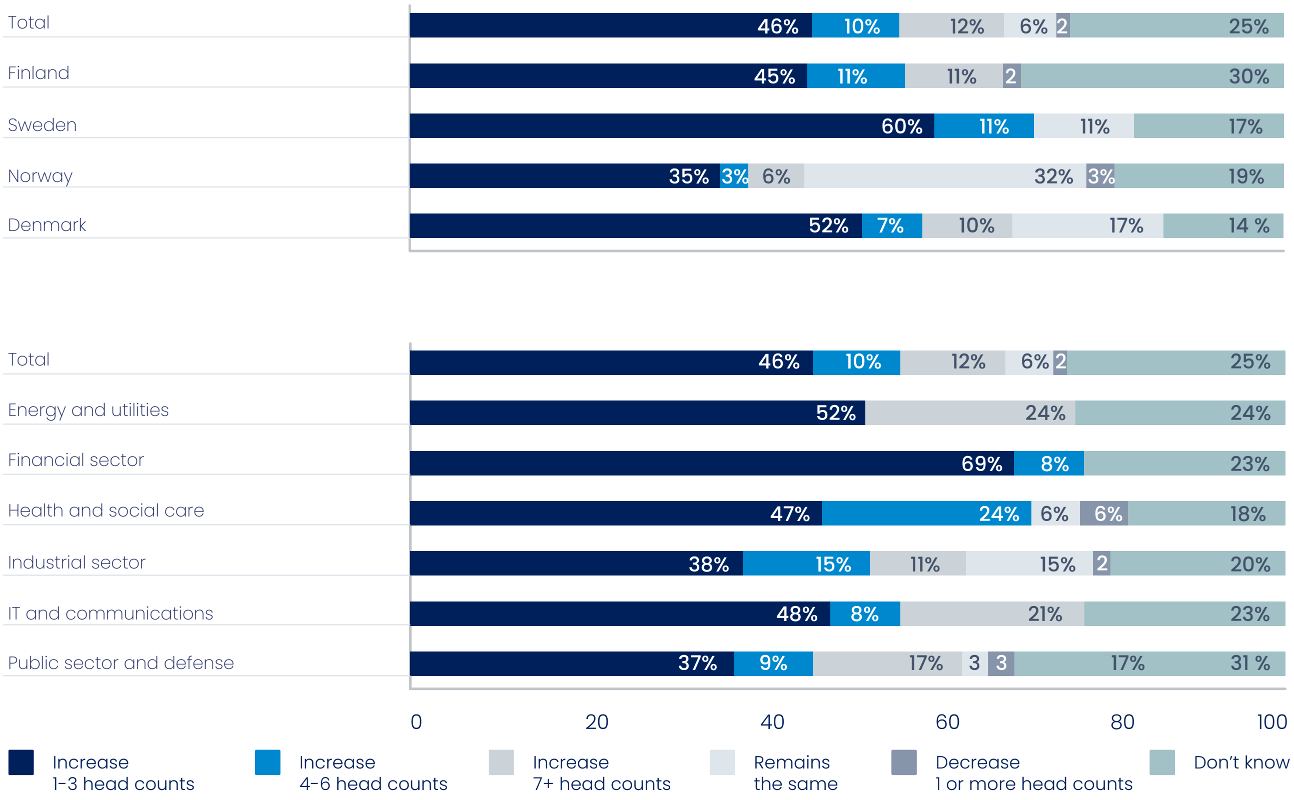
"Overall, ICT is outsourced, and therefore, the strategy for cybersecurity follows this ideology."

"Not enough in-house resources to allocate to cybersecurity efforts, nor budgets to hire additional full-time cybersecurity experts. No sufficient in-house expertise or competencies to cover all the cybersecurity topics."

"Outsourcing to provide 24/7 services and some special skills and knowledge."

Norwegian organizations will rely on external services, not on increasing internal headcount

Changes in internal headcount allocations for cybersecurity three years from now in the Nordic countries and industry sector



In Norway, the trend leans heavily towards outsourcing, likely due to limited resources and challenges in hiring in-house experts. Conversely, especially the larger organizations in Sweden tend to prioritize building in-house expertise. In Denmark, there's a modest intent to boost internal cybersecurity staffing, with minimal expectations also for growth in external headcount allocations.

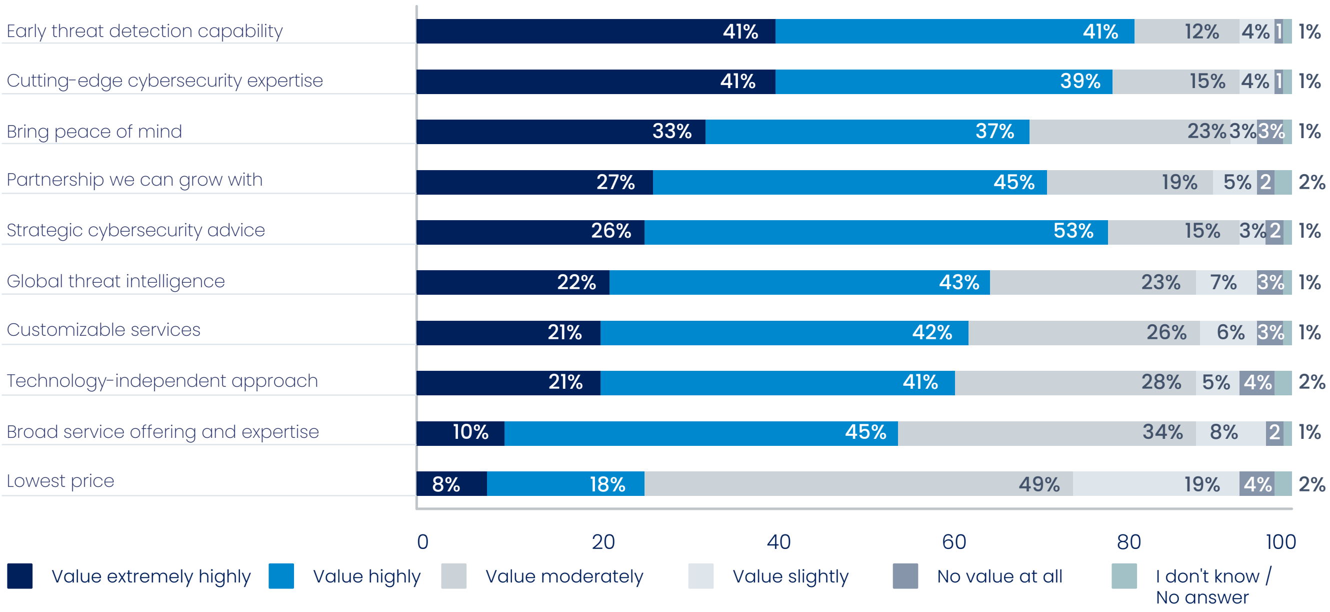
From an industry perspective, the energy and utilities and IT and communications sectors are keen on expanding their internal teams. Over 20% of these organizations aim to recruit seven or more cybersecurity specialists.

The financial and industrial sectors are most in favor of outsourcing two key competencies: over 50% of them intend to have **security monitoring and incident response** outsourced, and 40% plan to procure services for **threat intelligence and early warning**. Additionally, the financial sector shows a strong inclination to outsource **infrastructure security**.

Regardless of industry, very few respondents consider outsourcing **security awareness**. However, there's a clear challenge. Many organizations lack the educational resources paired with the necessary cybersecurity expertise to foster awareness. Given this limitation, it might be wise for these organizations to contemplate outsourcing as a viable solution.

Early threat detection capability and cutting-edge expertise are highly valued

How much do you value the following aspects in a cybersecurity service provider?



The value placed on **early threat detection** by cybersecurity service providers has seen a significant rise. This year, a remarkable 41% of respondents valued it extremely highly, a clear increase from 29% last year. Overall, it was valued highly or extremely highly by 82% of respondents, while last year similar appreciation was shown by 73%. Additionally, the capability to provide **peace of mind** saw an even more notable increase from 58% to 70%. At the same time, for example, the emphasis on **cutting-edge expertise** saw a decline from 97% to 80%.

Several factors could explain these shifts. One evident reason is the broader spectrum of respondents from diverse organizations and countries. The evolving nature of cyber threats and the imperative to manage incidents could be another contributing factor. Moreover, there seems to be a growing understanding of the benefits of investing in early detection – and the relief a competent service provider can offer in the often stressful realm of cybersecurity.

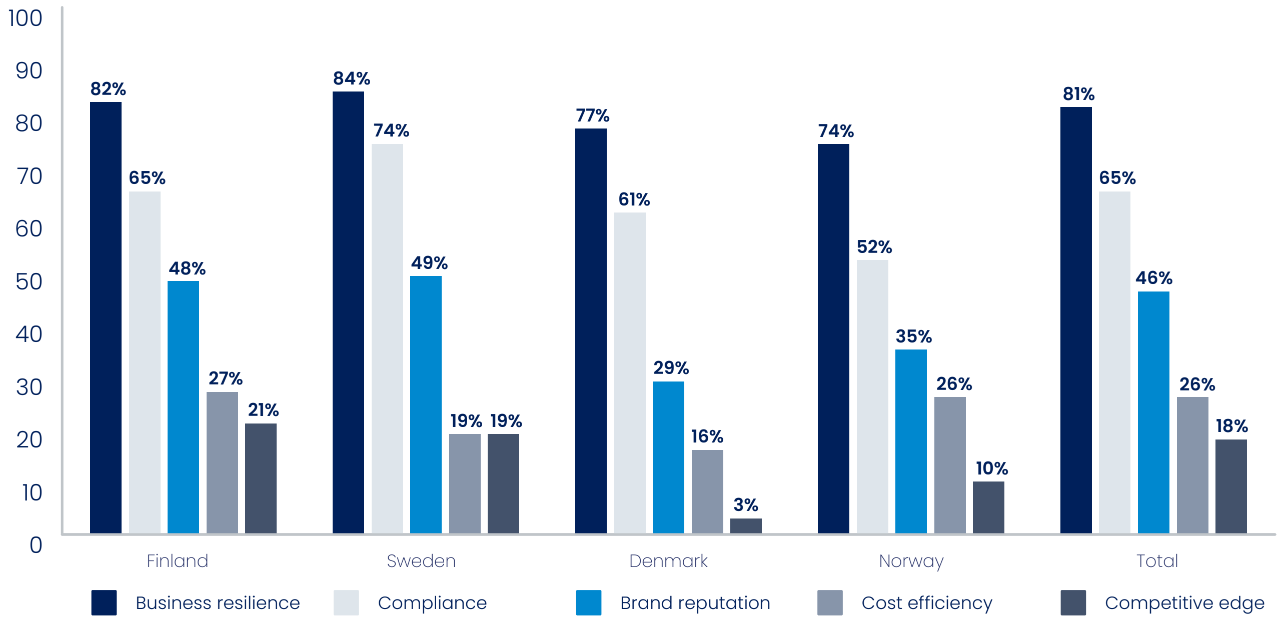
When comparing by country, Swedish and Finnish organizations emphasize the value of **strategic cybersecurity advice** the most, with 85% and 81%, respectively. In contrast, Danish and Norwegian entities place the highest value on early threat detection, with figures standing at 93% and 87%.

> There’s a clear causality between the perceived quality of risk management and confidence in the appropriate allocation of cybersecurity investments.

Investing in cybersecurity

Business resilience is the #1 driver of cybersecurity investments

What are the primary drivers of your organization's cybersecurity investments? Select 1–3 most important drivers.



For the first time, the survey also included a section about the drivers behind cybersecurity investments. The results indicate that **business resilience** is the predominant factor influencing investments across the Nordic region. In terms of **compliance** concerns, Sweden leads the pack, while Norway, with its respondents representing less regulated industries, lags behind.

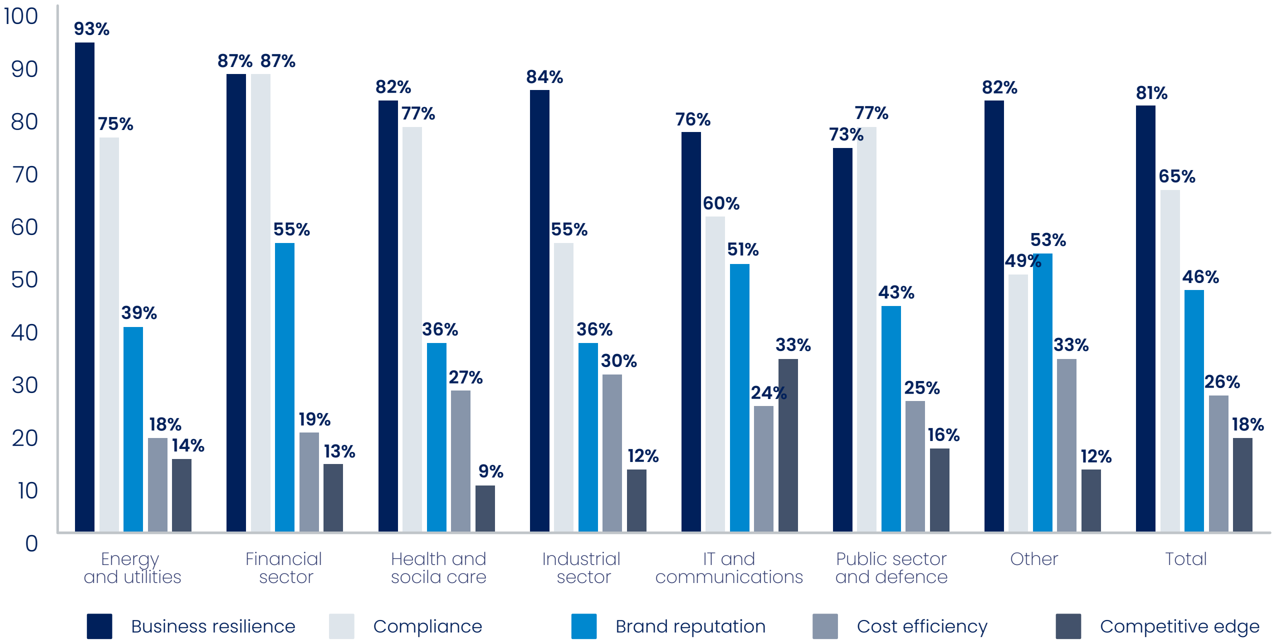
The importance of protecting the **brand reputation** resonates across all countries, but it's more pronounced in Finnish and Swedish organizations compared to their Danish and Norwegian peers. Interestingly, Denmark stands out for its limited focus on leveraging cybersecurity to gain a **competitive edge**, for example, by obtaining the ISO 27001 certification.

Despite economic challenges, the majority of organizations aren’t cutting back on their cybersecurity budgets. Yet, slight reductions were observed in Finland and Sweden.

On average, the total spend on cybersecurity decreased in 2023 compared to 2022, attributable to the participation of smaller companies in the survey. Consequently, there’s a rise in companies allocating less than 200,000 € for cybersecurity. The financial sector and companies boasting annual revenues exceeding 5 billion euros have the most substantial relative cybersecurity budgets.

Energy and utilities sector places an even greater emphasis on business resilience compared to the general average

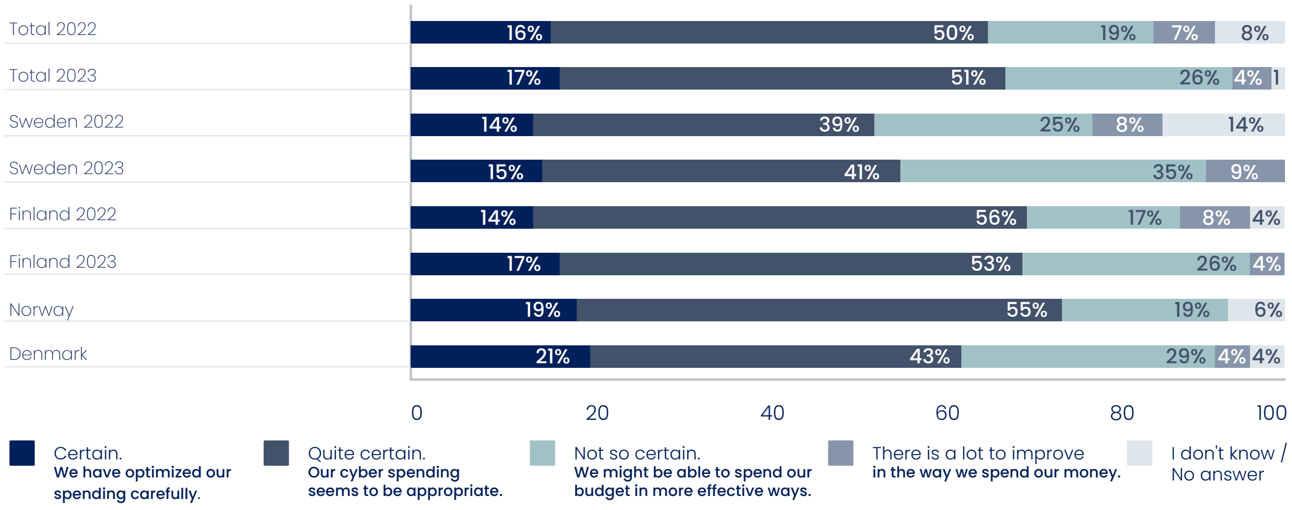
What are the primary drivers of your organization’s cybersecurity investments? Select 1–3 most important drivers.



When examining the drivers behind investments across various industries, distinct patterns emerge. **Business resilience** is most emphasized by organizations in the energy and utilities and financial sectors. **Compliance** stands out as the primary concern in the public sector and defense. **Brand reputation** gets the highest priority in the financial sector, IT and communications, and other non-classified industries.

Uncertainty about the effective allocation of cybersecurity budgets has grown slightly

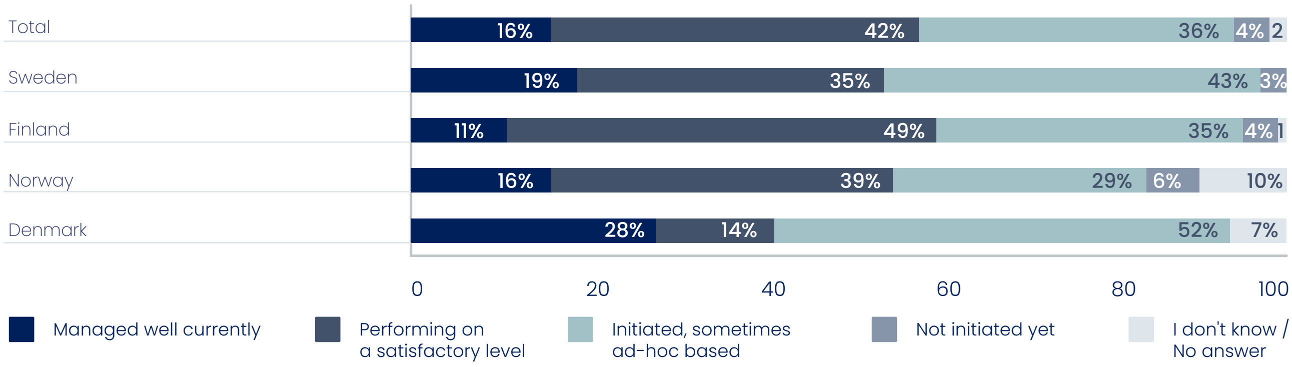
How certain are you that your organization's cyber spending is effectively used to mitigate business risks?



Uncertainty regarding security expenditures is slightly on the rise, with no explicit reasons provided. This could indicate that organizations have a grave need for risk management to alleviate uncertainty and guarantee optimal budget use. Swedish organizations, in particular, express concerns about their spending. In Norway, respondents are the most confident in their focus areas. In Finland, there is more uncertainty but the total share of certain and quite certain is the same. The share of respondents who think there is a lot to improve has halved.

Strong risk management boosts confidence in cybersecurity spending

Risk management - How would you describe the current state of the following capabilities of cybersecurity in your organization?



There's a clear causality between the perceived quality of **risk management** and confidence in the allocation of cybersecurity investments. Cross-tabulation (not shown here) reveals that on average, organizations with robust risk management practices are more confident in their spending: 30% believe their investments are well-optimized, with only 13% feeling uncertain. In contrast, among those with weaker risk management, only 10–15% are confident about their spending, while around 30% express uncertainty.

Nixu Cybersecurity Index

Nixu Cybersecurity Index 2023

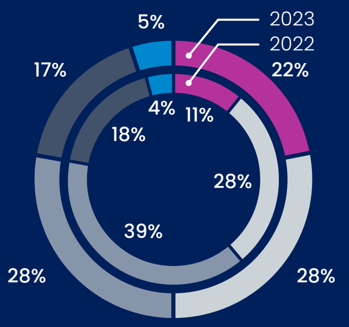
64,9

2022
67,3

Average of all respondents, scale 10-100

Half of the organizations were at a poor or deficient level in their cybersecurity maturity – this increased by 11% from 2022.

Similarly to last year, approximately one fifth (22%) of the organizations have reached a good or excellent level.



< 55 pts – POOR | 55 – 64,9 pts – DEFICIENT | 65 – 74,9 pts – SATISFACTORY | 75 – 84,9 pts – GOOD | > 85 pts - EXCELLENT

Danish and Norwegian companies' self-assessments indicate a slightly higher cybersecurity maturity compared to other northern European countries.

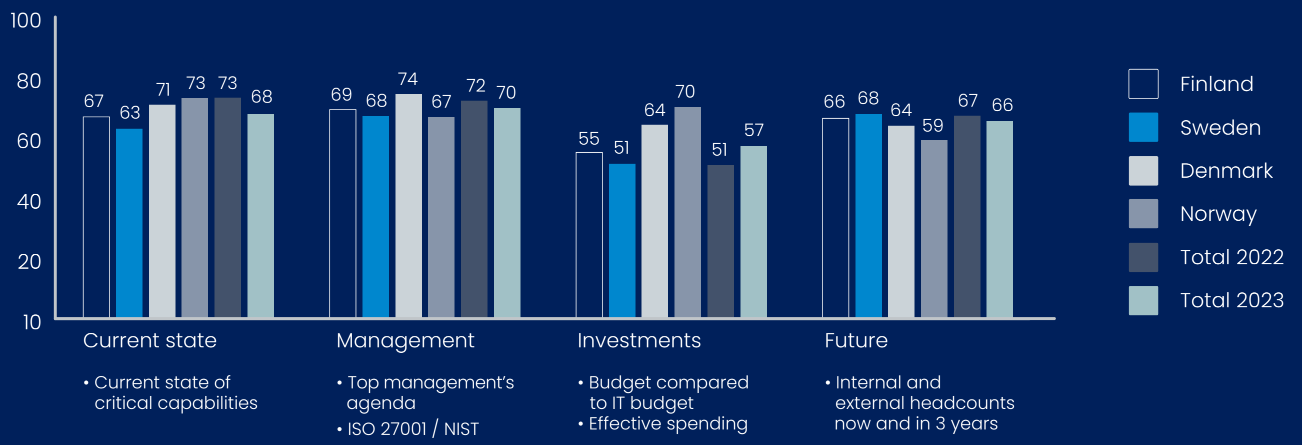
66,7
Denmark
SATISFACTORY
(2022: no data)

64,1
Finland ↓
DEFICIENT
(2022: 68)

70,0
Norway
SATISFACTORY
(2022: no data)

61,7
Sweden ↓
DEFICIENT
(2022: 63)

Even though Norwegian companies perform well, their headcount development looks very moderate



***Nixu Cybersecurity Index** measures the maturity level of organizations by evaluating the current state, management, investments, and future developments of cybersecurity. Each aspect is measured on scale 10-100. Number of respondents: 174.*

Key recommendations

The insights revealed by the second Nixu Cybersecurity Index display a mix of encouraging progress and areas of concern for northern European organizations. While some sectors show increased maturity, potentially due to heightened awareness and strategic outsourcing, challenges arise from regulatory compliance and the growing integration of AI in businesses.

On the positive side, we're pleased to see a doubling in respondent numbers, likely offering a clearer snapshot of the region's cybersecurity landscape. In accordance with its perceived relevance, business resilience emerged as the top driver for cybersecurity development.

On the negative side, the average Index score dipped from just satisfactory to deficient, with the proportion of underperformers doubling since 2022. Finland joined Sweden and descended to a deficient rank, while newcomers Norway and Denmark reached satisfactory levels, setting a new benchmark.

A closer look reveals a growing disparity between the best performing organizations and the rest of the Index respondents. If you want to give your organization's cybersecurity maturity a good boost, it's insightful to examine the practices that distinguish the best from the rest. Leading organizations have distinct approaches that set them apart.

Overall, the survey revealed that while organizations plan to allocate more resources to cybersecurity, they struggle with prioritization and resource constraints. Concerns about AI are evident, and regulations like NIS2, CER*, EUCS, CRA**, and DORA demand attention.
The shifting macroeconomic and geopolitical landscapes, including Sweden's potential NATO membership and Finland's recent inclusion, add to the uncertainty, potentially influencing more cautious evaluations.

Main differences between the best and the rest Best organizations reach a Cybersecurity Index of 75 or higher	**The Best**	**The Rest**
List risk management as one of the most critical capabilities	**58%**	**33%**
Have cybersecurity on executive management team's agenda	**76%**	**18%**
Report cybersecurity topics on board level	**71%**	**17%**
Have more than 2 people on their information security team	**66%**	**37%**
Spend less than 200 000€ on cybersecurity annually	**18%**	**40%**
Let cost efficiency be the primary driver for their cybersecurity investments	**16%**	**30%**
Allocate less than 5% of their ICT budget to cybersecurity	**5%**	**36%**

Percentages show how large proportion of the Best (or the Rest) belongs to the group

* CER = Critical Entities Resilience Directive
** CRA = European Cyber Resilience Act

How to tackle these challenges? The following considerations will set you on the path to enhanced cybersecurity maturity and reinforced business resilience.

1. When the battle for cyber talent intensifies, outsourcing emerges as the key solution.

Regardless of industry and country, almost every organization plans to grow its internal and external cybersecurity teams at least modestly. While the increase per organization seems minimal, the cumulative demand is substantial – too many are trying to fish in a very limited talent pool. The situation should encourage organizations to outsource cybersecurity more widely and expand outsourcing into areas considered until now purely in-house tasks, such as risk management, information security management, privacy and data security, and security awareness.

2. Compliance issues are best fought by a systematic and consistent security management approach.

As the deadlines to comply with new regulations approach, many organizations rush to take ad-hoc measures for each regulation to avoid penalties. There are, however, more efficient approaches. Having consistent cybersecurity management in place reduces the stress on resources and ensures adaptability to change. Furthermore, third-party audits and certifications validate compliance across the entire supply chain.

3. Effective risk management enhances the ability to make wise cybersecurity investments.

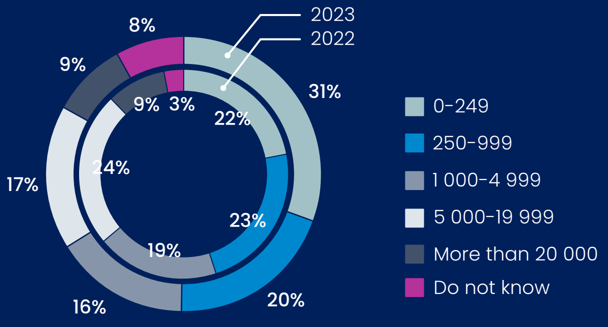
Determining areas of focus can be challenging while navigating the complex world of cybersecurity. Our advice is to first invest in risk management consultancy, which is the foundation for both strategic and operational choices. When you understand your vulnerability to cybersecurity threats in a dynamic threat environment, you can make smart investments for mitigation. Moreover, adhering to widely recognized security frameworks and obtaining certifications provide confidence and tools for decision-makers to balance their resource allocations.

Information about the 2023 survey and its respondents

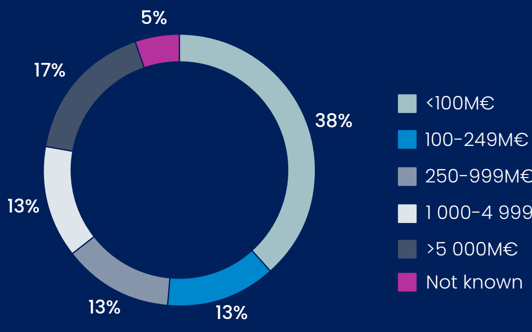
Share of respondents per country

58%	13%	9%	9%	12%
Finland	Sweden	Denmark	Norway	○ Other

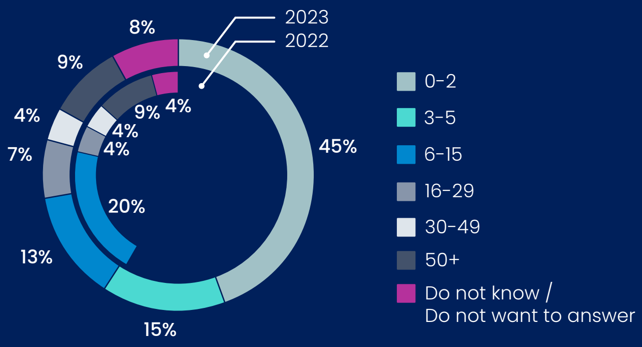
Number of employees



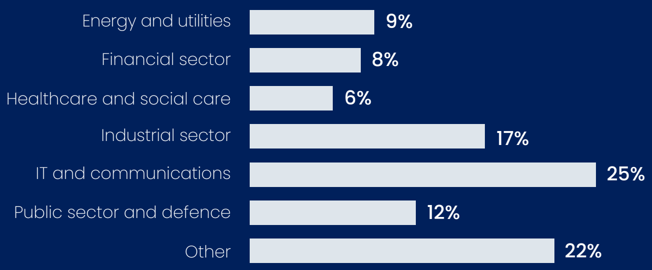
Annual revenue



Size of information security team



Industry



Data collection period:
June–August 2023

Data collection method:
Personal interviews and online survey

Number of respondents: 372

Experts behind the analysis:

Nixu: Henrik Engqvist, Eduardo Garcia, Peter Hellström, Ursula Heuman, Björn-Erik Karlsson, Niki Klaus, Edgar Kramer, Kimmo Kröger, Jan Mickos, Markku Rapo, Marek Rejmer, Veera Relander, Teemu Salmi Pietari Sarjakivi, Gorm Siiger, Minna Uitti, Kim Westerlund

DNV: Kirsti Eikeland

Method behind the Nixu Cybersecurity Index

The Nixu Cybersecurity Index is based on respondents' self-assessment responses in four categories: current state, management, investments, and plans for future developments in cybersecurity. Only capabilities that each respondent considers critical are counted. The score for each category is calculated separately, based on a set of questions, and the values vary from 10 to 100 points. The final Cybersecurity Index score is calculated by giving each category a different emphasis depending on its importance. The maximum score is 100, and the minimum is 10.

Scale: 100 points for each well-managed capability, 70 pts for satisfactory, 40 pts for ad-hoc operations, and 10 pts for not initiated.

CURRENT STATE OF CYBERSECURITY-RELATED ACTIONS IN ORGANIZATIONS

Emphasis
40%

The component score is counted as a mean of the identified critical capabilities: attack surface and vulnerability management, information security, identity and access management, infrastructure security, OT / factory IT security, privacy and data security, product and development security, risk management, security awareness, security monitoring and incident response, and threat intelligence and early warning.

Point scale for each capability: 10–100

MANAGEMENT OF CYBERSECURITY

Emphasis
20%

The component score is counted as a mean of three questions. Respondents were asked to assess whether cybersecurity is on the agenda of their executive management team and the board, and whether the organization follows the ISO 27001 standard / the NIST cybersecurity framework.

Point scale for each capability: 10–100

INVESTMENTS IN CYBERSECURITY

Emphasis
20%

The component score is counted as a mean of two questions. Respondents were asked about the cybersecurity budget's proportion of the whole ICT budget and the effectiveness of cyber spending in mitigating business risks.

Point scale for each capability: 10–100

FUTURE DEVELOPMENT OF CYBERSECURITY

Emphasis
20%

The component score is counted as a mean of two questions. Respondents were asked about the size of their information security team and the plans for internal and external headcount development in the next three years.

Point scale for each capability: 10–100

Nixu Cybersecurity Index, scale: 10–100

nixu cybersecurity.

Nixu is a cybersecurity services company that has been shaping the future through cybersecurity for over three decades. We make cyberspace a secure place and help our clients ensure business resilience with peace of mind. Nixu has Nordic roots, and we employ around 400 of the best professionals in Finland, Sweden, the Netherlands, Denmark, and Romania. Our experts are safeguarding the most demanding environments of some of the largest organizations in the world across all industries. Nixu shares are listed on the Nasdaq Helsinki Stock Exchange.

nixu.com

nixuoy nixucybersecurity company/nixu-oy @nixutigerteam | @nixuhq