nixu
cybersecurity.

CYBERSECURITY INDEX

Report 2022

Table of contents

Introduction

Nixu has a passion for cybersecurity. For more than 30 years Nixuans have worked towards building a more secure society, and during those years the field of cybersecurity has evolved and changed significantly.

These times of intense digitalization have required for all organizations to develop and assess their readiness to respond to cybersecurity threats. Some have taken this task more seriously and they are well on track with securing their digital operations. Others still have a long way to go in order to mitigate the cybersecurity risks we all face.

To go beyond assumptions and to truly understand how maturely organizations are handling their cybersecurity, Nixu decided to launch the annual Nixu Cybersecurity Index. It's a study that measures cybersecurity maturity in Northern European organizations by evaluating four aspects of cybersecurity performance: current state, management, financial investments, and future development plans.

These times of intense digitalization require all organizations to develop and assess their readiness to respond to cybersecurity threats. Some have taken this task more seriously, and they are well on track with securing their digital operations. Others still have a long way to go in order to mitigate the cybersecurity risks we all face.

In this report, we will dive deeper into the survey results and present our key findings and conclusions based on the data. You will find insights about cybersecurity trends and key capabilities, and how companies tend to manage internal and external competences within cybersecurity. We will also look at cybersecurity budgets. Finally, we will present the Nixu Cybersecurity Index in more detail, looking at the four aspects of cybersecurity performance.

We hope this report offers you interesting insight into the current state of cybersecurity and gives food for thought when it comes to enhancing your own cybersecurity efforts. Keeping our digital surroundings safe is everyone's business, and we are all responsible for making our own contribution towards the common good.

Key findings

1 As many as 39% of organizations are on a poor or deficient level in cybersecurity

In this study, 22% of organizations assessed their cybersecurity maturity to be on a good or excellent level. Only 4% of organizations have reached an excellent level in cybersecurity.

Low budgets and inefficient budget spending are the key detractors of the overall score. While the average score for other aspects (current state, management, and future development) is 67–75, the average score for financial investments is 54.

2 Supply chain security taking over from ransomware as hottest topic in cybersecurity

Ransomware was identified as the hottest cybersecurity topic during the recent 12 months.

However, looking at the next 12 months, cybersecurity decision makers expect supply chain security to take over as the #1 topic in cybersecurity. Supply chain security is, of course, an extensive topic and includes a lot of security concerns. Cybersecurity is just one aspect, albeit an important one.

3 Security awareness considered most critical capability – risk management assessed surprisingly low in importance

Security awareness is identified as the most critical cybersecurity capability, and it is also the most important capability to strengthen in the next 12 months.

Organizations assess risk management as a surprisingly uncritical capability. However, more than a third of the respondents (38%) say that risk management is not well initiated in their organization.

4 One out of four organizations (26%) is not spending their budget in an effective way

Two thirds (66%) of the respondents are certain or quite certain that their cybersecurity spending is optimized and appropriate.

Meanwhile, 26% are less certain and they feel their cybersecurity budget could be spent more effectively.

5 Organizations value quality strongly over price

When it comes to cybersecurity, it's without exception that respondents say quality is more important than a low price.

A service provider's deep expertise in cybersecurity is valued highly or extremely highly by 97% of respondents.

Lowest price is considered least important, although more than one fifth (21%) still give it high or extremely high value.

Supply chain security is the hottest topic in cybersecurity within the next 12 months.

Trending topics in cybersecurity

Ransomware #1 cybersecurity topic in 2022, but Supply Chain Security is increasing importance

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

- Ransomware
- Phishing
- Operational Technology Security
- Vulnerability Management
- Supply Chain Attacks

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

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

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

- Supply Chain Security
- Phishing
- Cloud Security
- Operational Security
- Identity and Access Management
- Security Awareness

"Human-centered security awareness"

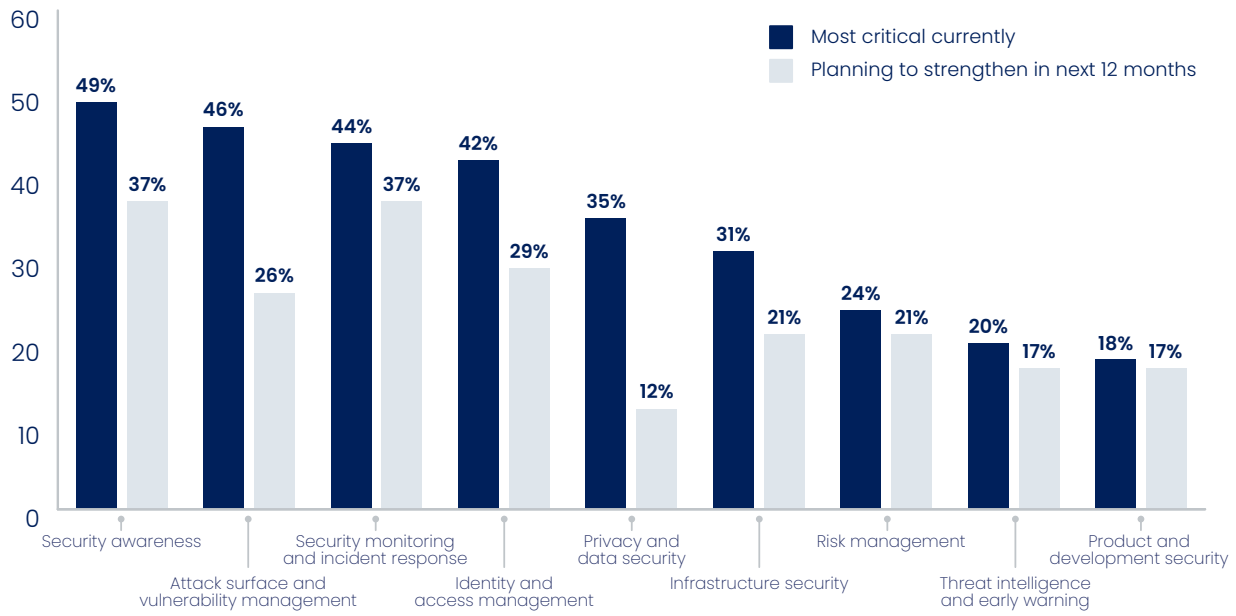
"Business interest in how security measures are created and managed is rising very much"

"Cyber resilience (prevention, detection and recovery) and supply chain security"

Key capabilities in cybersecurity

Security awareness considered most critical capability – risk management assessed surprisingly low in importance

Assessment of most critical capabilities currently and development plans for the next 12 months



Security awareness is clearly an important topic, as it is currently considered both critical and a top capability that organizations want to strengthen in the future. Consistent organization-wide efforts to increase security awareness help enhance the organization's security culture and lead to improved security posture and more resilient business. With good training and continuous communication, employees can be the organization's strongest link in cybersecurity to fight against constantly evolving cyber threats.

Attack surface and vulnerability management is a topic where we can see a clear gap between how critical it is considered currently, and how likely the organization is to further develop it during the next 12 months. Since attack surface and vulnerability management is typically included in outsourcing contracts, it could be that organizations have made the conscious choice to leave this area to their outsourcing partners and not put effort into strengthening the capability internally.

Privacy and data security is another area where organizations do not have plans in place to strengthen their capabilities, although it's currently assessed to be relatively critical. This could be because GDPR legislation has forced European organizations to grow their privacy maturity already. Privacy and data security may have become commodities that do not require heavy focus going forward. This, however, harbors the risk of organizations not giving enough attention to protecting sensitive data.

Risk management is currently identified as a critical capability by relatively few cybersecurity decision makers. Nor are very many planning on strengthening their organization's skills in the area in the future. This comes as a surprise considering that risk management should be at the core of cybersecurity in every organization.

In fact, it seems that cyber risks are not a part of corporate risk assessment, and that cyber risk management is disconnected from corporate risk management. Key challenges stem from corporate risk managers who are unfamiliar with cyber risks and subsequently reluctant to assume responsibility for them. Conversely, cybersecurity risk managers who are unfamiliar with corporate risks are only willing to look at risk management from the IT security perspective.

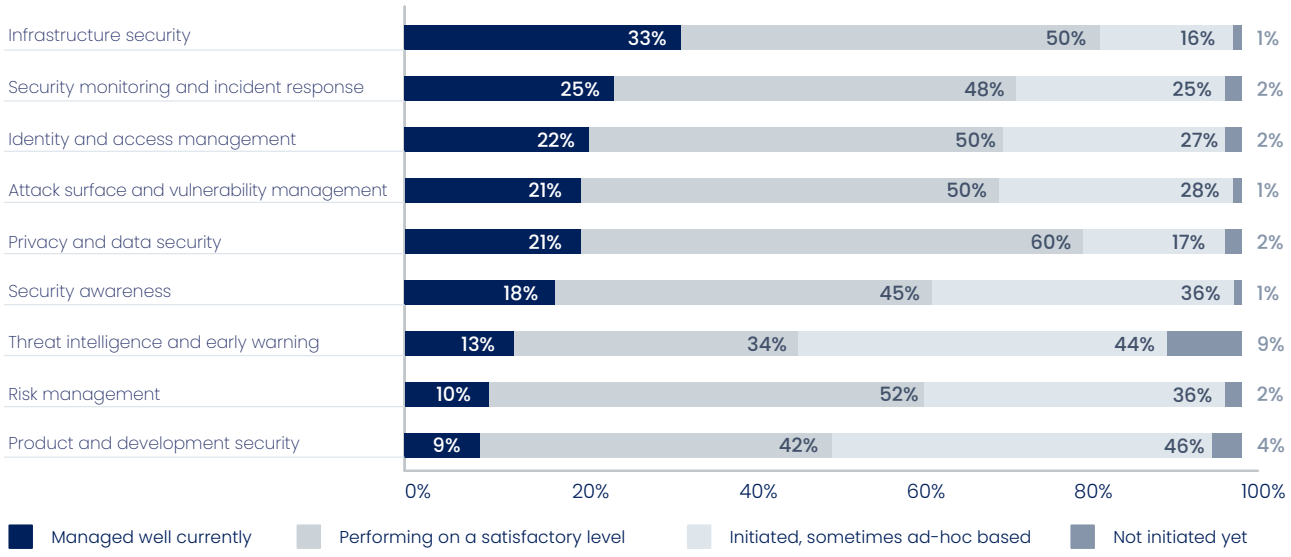
One way to mitigate the situation would be for cybersecurity risk managers to adopt corporate risk methodology. The goal could be to combine cybersecurity and corporate risk handling within the next 1-2 years.

Overall, the capabilities that respondents identified as most critical currently are also the capabilities they plan to strengthen further in the upcoming months. As a rule, however, there are fewer respondents saying that they have plans to strengthen their capabilities further than there are respondents claiming for the capability to be critical. Therefore, it seems that some organizations assess their capabilities to be high enough already, or they simply lack the resources to develop these capabilities further.

Current state of cybersecurity

Infrastructure security is the best managed cybersecurity capability in Northern Europe

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



Infrastructure security is usually what first comes to mind when people think about information security. Organizations have invested in it for a long time, and infrastructure security is seen as the strongest capability – one third of all respondents say that it's an area that is managed well.

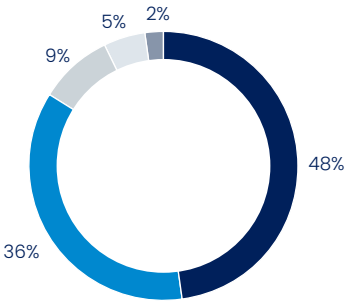
Organisations also seem quite confident that the management of privacy and data security issues is at a good level.

More than a third of all respondents (38%) say that risk management is not well initiated, and only 10% say it is managed well. This is an alarming result considering the fact that risk management is also not identified to be one of the most critical capabilities currently, nor is it among the top capabilities to develop going forward.

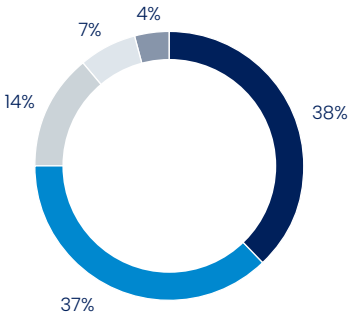
Long-term planning in risk management would be much more efficient than putting one's efforts into ad hoc development. Unfortunately, the latter seems to be what many organizations are doing. Risk management should be the foundation of cybersecurity in every organization, and the results in this study strongly suggest that its importance is neglected by many organizations.

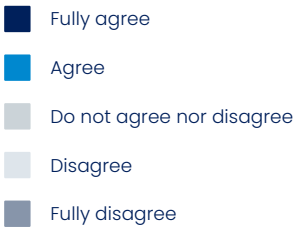
Cybersecurity has reached the executive management team regardless of country or industry

Cybersecurity is on our executive management team's agenda



Cybersecurity topics are reported on the board-level in our organization





Topics related to cybersecurity are on the executive team's agenda and they are reported also to the board-level in most organizations. One reason for this is the leaders' growing interest in cybersecurity threats. This has been boosted by, for example, the war in Ukraine and the increasing number of cyberattacks visible in the media.

Swedish organizations show lower cybersecurity maturity compared to other countries

Percentage of respondents who feel the capability is managed well

	Total	Finland	Sweden	Other countries
Infrastructure security	33%	36%	22%	41%
Security monitoring and incident response	25%	29%	11%	36%
Identity and access management	22%	28%	8%	29%
Attack surface and vulnerability management	21%	23%	11%	32%
Privacy and data security	21%	20%	14%	33%
Security awareness	18%	17%	16%	24%
Threat intelligence and early warning	13%	10%	3%	41%
Risk management	10%	13%	5%	10%
Product and development security	9%	10%	3%	14%

0–10% 11–20% 21–30% 31–40% 41% or more

According to the self-assessment of respondents, the organizations in other countries show higher cybersecurity maturity than Finnish and Swedish organizations in nearly all capabilities. In fact, in this study, Swedish organizations show lower cybersecurity maturity than other countries.

One possible reason for lower maturity in Sweden might be that comprehensive security thinking is more relevant for e.g. Finland due to its geopolitical situation. Another reason could be the fact that Finnish companies are more used to outsourcing their cybersecurity resources, whereas Swedish companies, to a larger degree, prefer having full control in-house.

Top concerns related to cybersecurity

Weak cybersecurity causes many concerns. The topics that worry respondents the most are related to the organizations' own operations, their customers' business, possible reputational damage, and the leakage of sensitive data.

37% Cyber threats may harm our operations / production

24% Cyber threats may harm our customers' daily business

24% Cybersecurity issues may harm our corporate image

23% Intruders can access our business data

16% Uncertainty in the geopolitical situation leads to cyber threats to our business

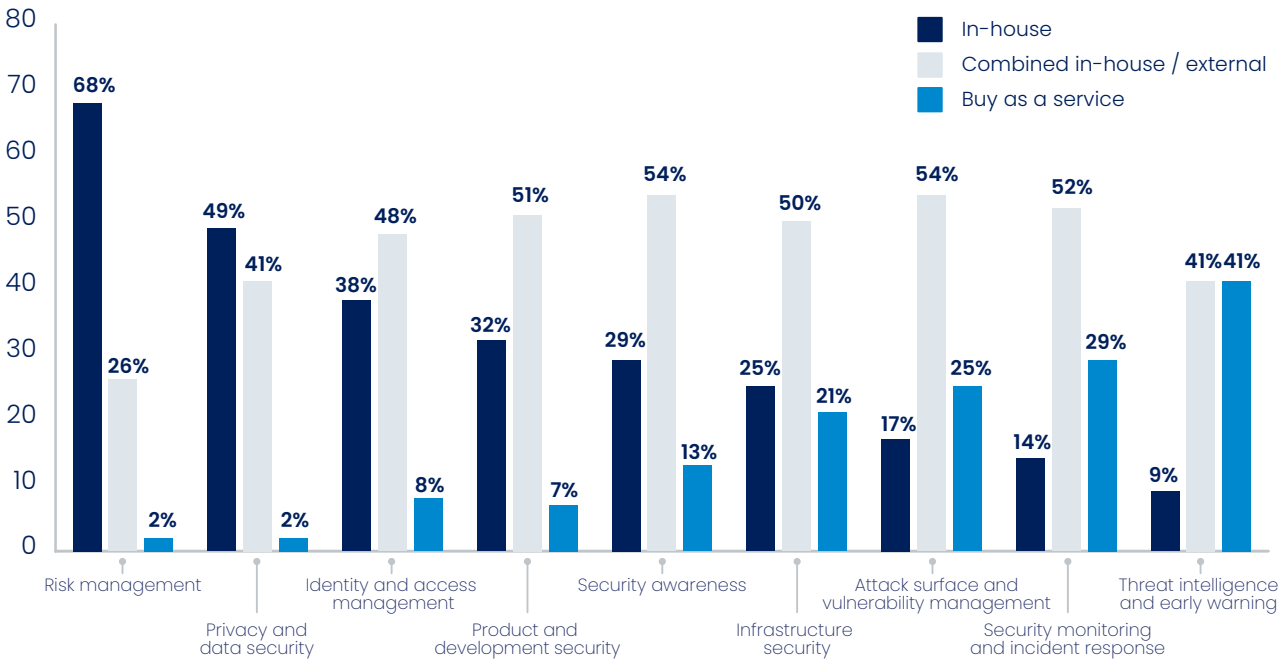
16% We do not have enough skills and competencies to manage all relevant topics in cybersecurity

> **Many organizations would benefit from putting extra effort into enhancing their risk management capabilities.**

Managing competences

Risk management as well as privacy and data security are the most common in-house capabilities

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



Almost all cybersecurity capabilities are usually covered by a mix of in-house and external skills. More than 40% of respondents say that a combination of the two is the preferred option for all capabilities except risk management, which is clearly considered an in-house competence in most organizations (68%).

As stated earlier, the results also show 38% of the respondents say that risk management is not well initiated, and only 10% say it is managed well. It seems that many organizations would benefit from putting extra effort into enhancing their risk management capabilities. If it cannot be done well in-house, organizations should consider finding an outsourcing partner to help them with cybersecurity risk management.

A combination of in-house and external skills is the preferred option to cover cybersecurity capabilities.

Another capability that is more commonly covered in-house is privacy and data security (49%). This is most likely due to the relatively recent requirements for GDPR compliance which has led to many organizations investing more heavily in privacy maturity.

The capability that respondents are most likely to buy as a service is threat intelligence and early warning (41%). More than a quarter of the respondents also say that they will outsource security monitoring and incident response (29%) as well as attack surface and vulnerability management (25%).

Looking at different industries, IT companies generally have more in-house capabilities than other industries. On average, 39% of their cybersecurity capabilities are handled internally, whereas the average for all other industries is 30%.

Companies within the financial sector are more likely to handle in-house the competences central to their business, such as privacy and data security (86%), risk management (77%) and security awareness (55%).

Managing competences is a continuous challenge for companies

KEY REASONS FOR **IN-HOUSE COMPETENCES**

"You cannot outsource responsibilities"

"Combining security with business understanding"

"Growth requires internal competences and implementation"

"External requirements (e.g. law, regulation)"

KEY REASONS FOR **COMBINED APPROACH**

"Optimal balance between efficiency and internal competencies"

"Services support our in-house competencies"

"Flexibility"

KEY REASONS FOR **OUTSOURCING**

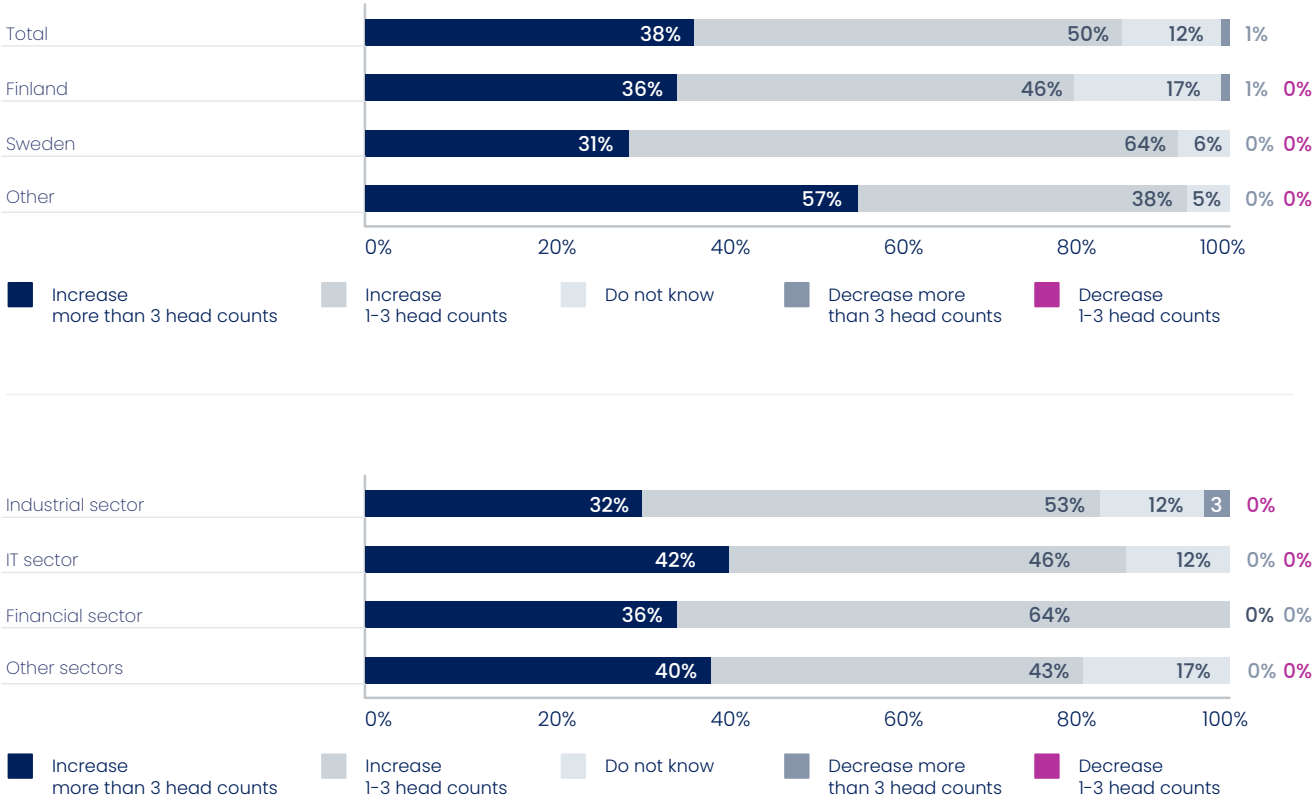
"Skills requirements – impossible to have in-house"

"We get the best people by outsourcing"

"Company's strategic decision"

Internal headcount allocation for cybersecurity is expected to increase

Changes in internal headcount allocations for cybersecurity three years from now



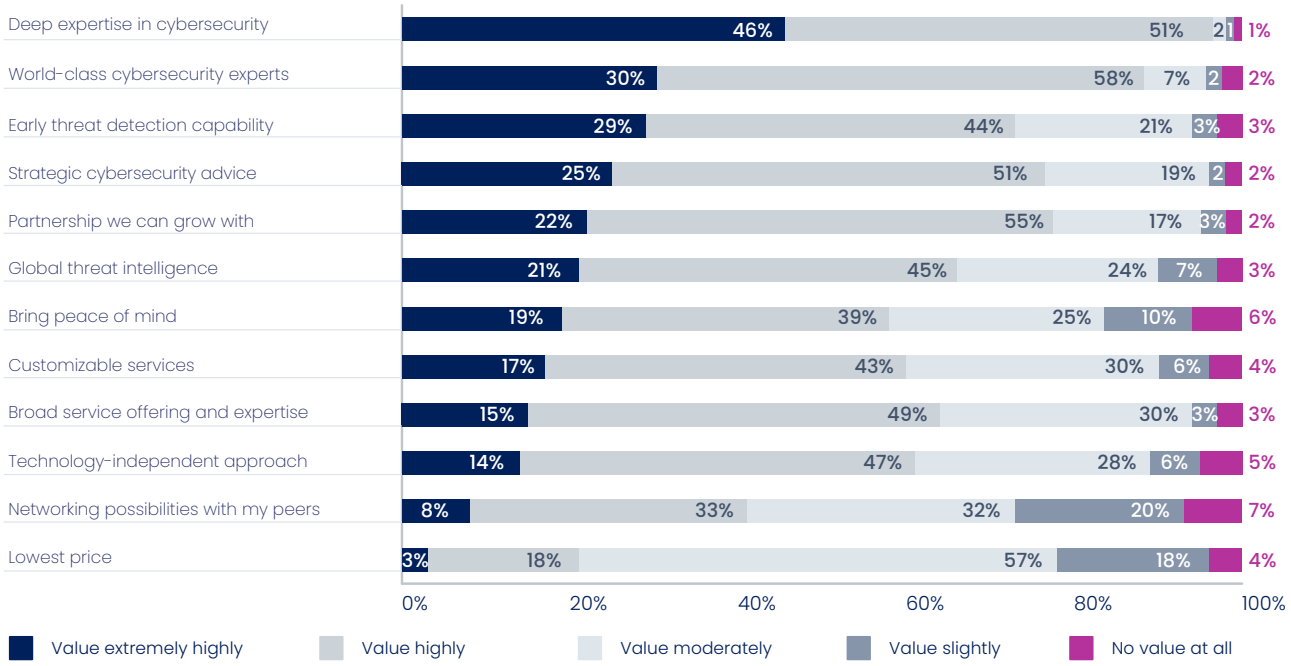
Internal headcount allocation for cybersecurity is expected to increase in the next few years across all countries and industries. Very few respondents expect the allocation to decrease, which indicates that organizations have understood the critical role and increasing importance of cybersecurity. This is especially visible in the financial sector, where all respondents expect to hire more cybersecurity professionals.

Finding talent to hire may prove to be easier said than done. There is a global cybersecurity skills shortage, and organisations are likely to end up competing over the same talent. Instead of trying to secure the perfect cybersecurity expert for your in-house team, it might make more sense to outsource cybersecurity capabilities. This way you will have the right skillset available to you at the right time – as will everyone else. Under these circumstances, organisations will benefit from seeking external assistance.

NOTE: Industry results are only shown for industries with over 30 respondents. Here, the industrial sector also includes the materials industry, and the financial sector includes the real estate industry.

Cybersecurity service providers are expected to have deep cybersecurity expertise

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



Deep expertise and world-class experts rank highest when considering cybersecurity service providers' most valuable assets. The results indicate that cybersecurity decision makers generally value quality over low price.

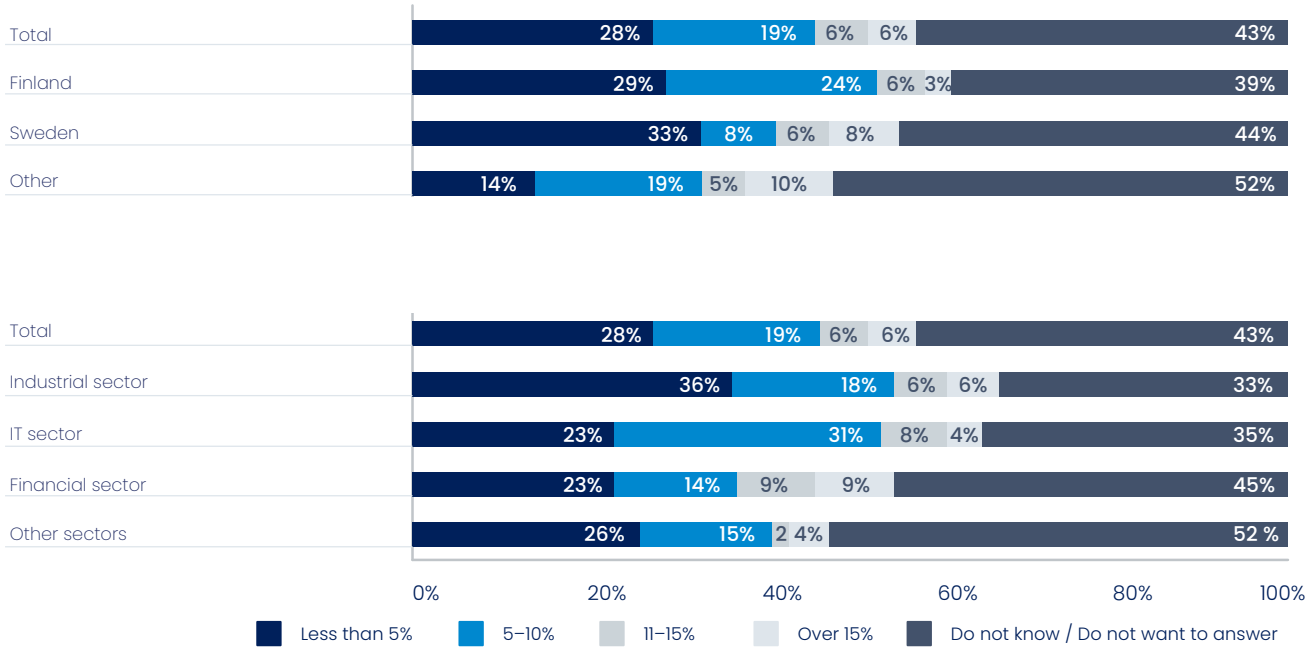
However, more than one fifth of respondents (21%) still stated that they value the lowest price highly or extremely highly.

Many companies are not spending their cybersecurity budget as effectively as they could – and should.

Investing in cybersecurity

Cybersecurity spending is expected to grow

Cybersecurity budget's proportion of the whole ICT budget



When annual revenue exceeds 1000M euros, cybersecurity spend tends to exceed 1M euros. Comparing against the organization's overall ICT budget, many companies (28%) spend less than 5% on cybersecurity.

Companies within the financial sector have the biggest cybersecurity budgets. They also seem to invest the highest share of their ICT budget in cybersecurity. In the financial sector, cybersecurity is part of the core business and investments are higher than in other sectors.

In the financial sector, cybersecurity investments are higher than in other sectors.

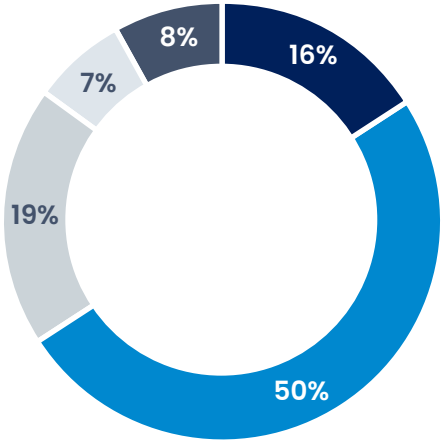
NOTE: Industry results are only shown for industries with over 30 respondents. Here, the industrial sector also includes the materials industry, and the financial sector includes thereal estate industry.

Overall, cybersecurity spending is currently quite modest. Considering that most organizations are planning to increase their internal headcount allocations for cybersecurity, also spending is expected to grow in the next few years.

The results also show that many companies (26%) are not spending their cybersecurity budget as effectively as they could – and should. Making changes to budget allocations could ease the pressure to increase cybersecurity budgets and lead to better mitigation of business risks.

One out of four respondents says that their organization is not spending their cybersecurity budget in an effective way.

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



- Certain
  We have optimized our spending carefully
- Quite certain
  Our cyber spending seems to be appropriate
- Not so certain
  We might be able to spend our budget in more effective ways
- There is a lot to improve in the way we spend our money
- Do not know / Do not want to answer

Nixu Cybersecurity Index

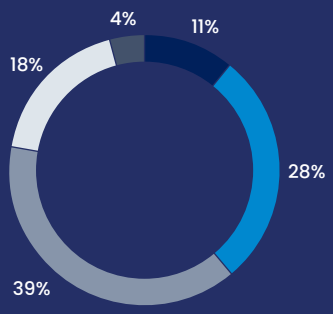
Nixu Cybersecurity Index 2022

67

Average of all respondents, scale 10-100

22% of organizations reach a good or excellent level in cybersecurity – 39% are at a poor or deficient level

Only 4% of organizations have reached an excellent level in cybersecurity



Poor | Deficient | Satisfactory | Good | Excellent

< 55 pts – POOR | 55 – 65 pts – DEFICIENT | 65 – 75 pts – SATISFACTORY | 75 – 85 pts – GOOD | > 85 pts - EXCELLENT

Swedish companies' self-assessment shows lower cybersecurity maturity compared to other countries

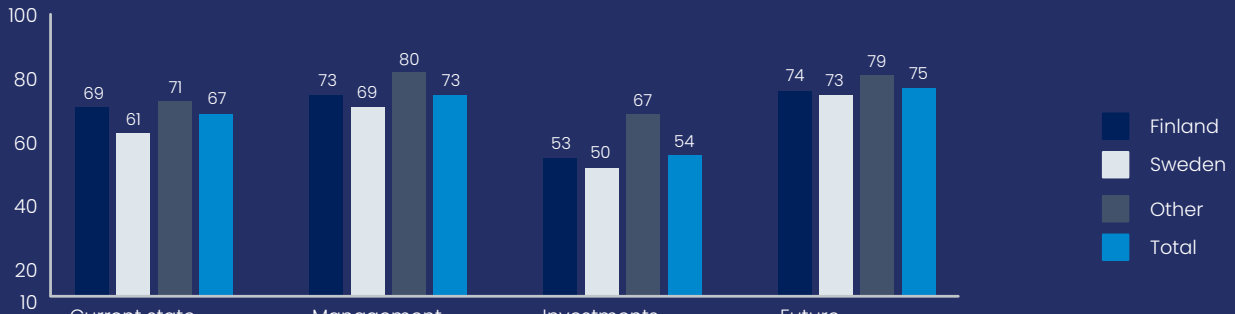
68 **Finland**
SATISFACTORY

63 **Sweden**
DEFICIENT

73 **Other**
SATISFACTORY

67 **All countries**
SATISFACTORY

Low budgets and inefficient budget spending are the key detractors of the overall score



Current state
- Current state of critical capabilities

Management
- Top management's agenda
- ISO 27001 / NIST

Investments
- Budget compared to IT budget
- Effective spending

Future
- Internal and external headcounts now and in 3 years

Nixu Cybersecurity Index *measures the maturity level of organizations by evaluating the current state, management, financial investments, and future developments of cybersecurity. Number of respondents: 112.*

Key takeaways

Our intention with the Nixu Cybersecurity Index is to shed light on the current state of cybersecurity in Northern European organizations. We measure cybersecurity maturity by evaluating four aspects of cybersecurity performance: current state, management, financial investments, and future development plans.

This is the first survey we have conducted using this approach, and based on the results, the average maturity score in 2022 is 67. This is barely satisfactory on the 10–100 scale. The average score for Swedish organizations was even lower, 63, which stands for a deficient result. Overall, the results show that 39% of Northern European organizations are on a poor or deficient level in their cybersecurity maturity.

The survey also reveals that supply chain security is becoming the next top concern, focus on risk management is surprisingly low, deep expertise is the most valued quality in service providers, and cybersecurity spending may not be optimal in many organizations.

Based on the results, we recommend all organizations to consider the following aspects on their cybersecurity development journey:

1. The rise of ransomware is best fought by combining technical measures with security awareness

Improving security culture through consistent organization-wide programs contributes to business resilience towards cyber threats. With good training against ransomware and phishing emails, employees can be the organization's strongest link in cybersecurity. However, security awareness is not enough to fully mitigate risks. The best way to fight the rise of ransomware is to combine technical measures and security awareness.

2. Risk-based decisions help ensure effective cybersecurity management and spending

The survey results indicate that cybersecurity has been managed more as a technology item than an integral part of corporate risk management. However, cybersecurity is all about risk management, and it should be addressed as a business issue. Initiating a proper information security management system would help organizations make fact-driven and risk-based decisions on cybersecurity management and spending.

3. Geopolitical developments increase the need for comprehensive security thinking

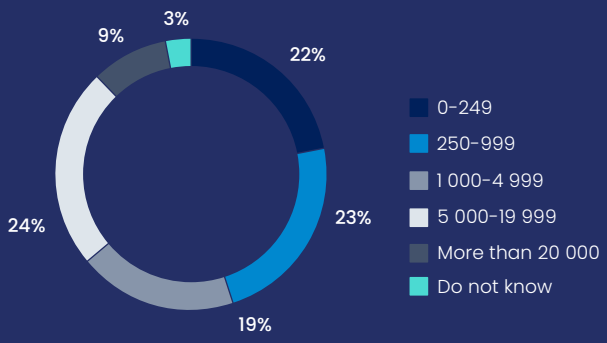
Global geopolitics affect not only military and governmental organizations – they mold the reality which we all live in, regardless of industry or geographic location. Therefore, mitigating cybersecurity risks is everyone's business. Under these circumstances, any organization would benefit from seeking relevant, accurate, and actionable insight to better understand their threat landscape.

Information about the survey

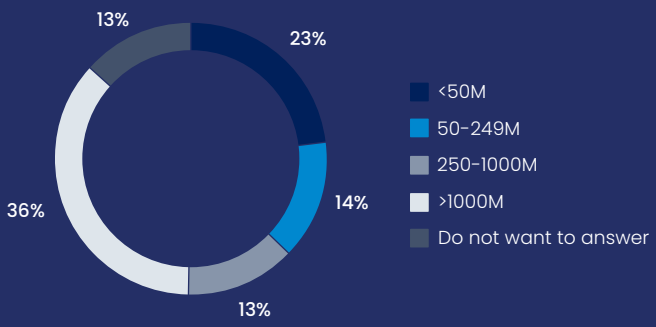
Country

59%	25%	4%	8%	4%
Finland	Sweden	Denmark	Netherlands	Other

Number of employees

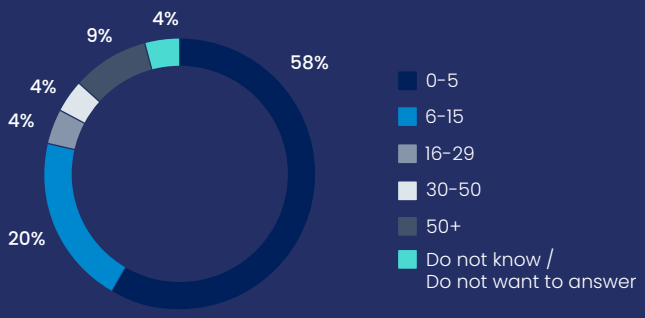


Annual revenue

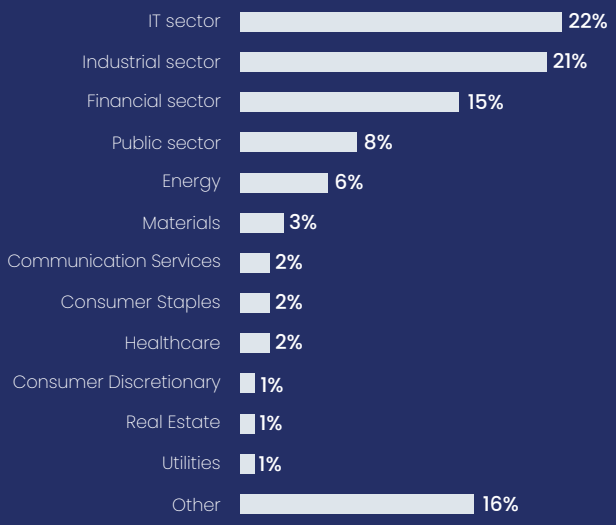


Size of information security team

How many people are employed full-time for the information security team in your organization?



Industry



Data collection period:
September–October, 2022

Data collection method:
Personal interviews and online survey

Nixu experts behind the analysis:

Peter Hellström, Ursula Heumann, Björn-Erik Karlsson, Jan Mickos, Valtteri Peltomäki, Markku Rapo, Pietari Sarjakivi,

Number of respondents: 180

Method behind the Nixu Cybersecurity Index

The Nixu Cybersecurity Index is based on respondents' self-assessment responses in four categories: current state, management, financial investments, and plans for future developments in cybersecurity. The score for each of the four categories is calculated separately, based on a number 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 Cybersecurity Index score is 100 and the minimum is 10.

CURRENT STATE OF CYBERSECURITY-RELATED ACTIONS IN ORGANIZATIONS

Emphasis
40%

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

Point scale for each capability: 10-100

MANAGEMENT OF CYBERSECURITY

Emphasis
20%

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 question: 10-100

FINANCIAL INVESTMENTS IN CYBERSECURITY

Emphasis
20%

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 question: 10-100

FUTURE DEVELOPMENT OF CYBERSECURITY

Emphasis
20%

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 question: 10-100

Nixu Cybersecurity Index, scale: 10-100

nixu
cybersecurity.

Nixu is a cybersecurity services company on a mission to keep the digital society running. Our passion is to help organizations embrace digitalization securely. Partnering with our clients, we provide practical solutions for ensuring business continuity, an easy access to digital services, and data protection. We aim to provide the best workplace to our team of about 400 cybersecurity professionals with a hands-on attitude. With Nordic roots, we serve enterprise clients worldwide. Nixu shares are listed on the Nasdaq Helsinki stock exchange.

nixu.com

nixuoy @nixutigerteam | @nixuhq company/nixu-oy