Survey results B2B

Ordered by NGO Secure, for KnowCyber project, financed by e-Governance Academy

February – March 2025.

WELCOME

Findings of the assessment of cyber hygiene practices in Small and Medium Enterprises (SMEs)

STARSUP

Based on the presented data, the following conclusions can be drawn:

Low awareness of cyber hygiene

The majority of respondents (**76.5%)** are not familiar with the concept of cyber hygiene, which indicates a serious lack of basic knowledge about digital security. This issue is particularly pronounced in micro and small enterprises, where the percentage of uninformed respondents is significantly higher compared to **medium-sized and large companies**.

Insufficient implementation of cybersecurity measures

Although most respondents practice a moderate level of cyber hygiene (**53.3%**), only 1.7% achieve a high level of protection. A large share of employees **do not use key tools** such as two-factor authentication, password managers, or data encryption, which increases the risk of cyberattacks**.**

Weak policies and incident reporting

Although **67.5%** of companies have some form of cyber hygiene policies in place, **these policies are not sufficiently clear nor consistently enforced.** Additionally, **34.4%** of employees **are not familiar with cybersecurity incident** reporting procedures, which may result in many threats remaining undetected or unreported.

Insufficient investment in cybersecurity

Only **23.2%** of companies **allocate adequate resources to cybersecurity**, while **13.9%** invest far less than necessary. The lack of qualified personnel (**31.8%)** and limited management support (**20.9%)** further hinder efforts to improve cyber hygiene**.**

Based on the presented data, the following conclusions can be drawn:

Software and password updates

More than **60% of employees update software only when prompted by** the system, while **21.9% rarely or never update their work devices**, creating opportunities for cyberattacks. Additionally, although **54.3% of employees have a policy requiring regular password changes**, many ignore it, further reducing the overall level of data protection.

Cybersecurity training is rare and underdeveloped

A total of **85.4% of respondents have never undergone cybersecurity training**, while those who have find the trainings useful but in need of further improvement. Interestingly, **83.4% of respondents do not consider such training necessary**, indicating low awareness of risks and the potentially severe consequences of cyberattacks.

Greatest interest in data protection

The majority of respondents **(42.7%) are interested in improving the protection of personal and business data**, while topics such as device security and recognizing cyberattacks are lower priorities. This highlights the need for additional training on threat identification, especially **phishing attacks**, which most respondents still struggle to recognize.

Training potential for reducing risk

A total of **87.4% of respondents believe that additional training would help reduce the risk of cyber incidents,** although its effectiveness depends on a combination of education and technical security measures. The most in-demand training formats are **interactive in-person workshops (36.8%) and video lessons that can be followed in one's own time (34.8%).**

STARSUP

Methodology and working approach

STARSUP

INTRODUCTION

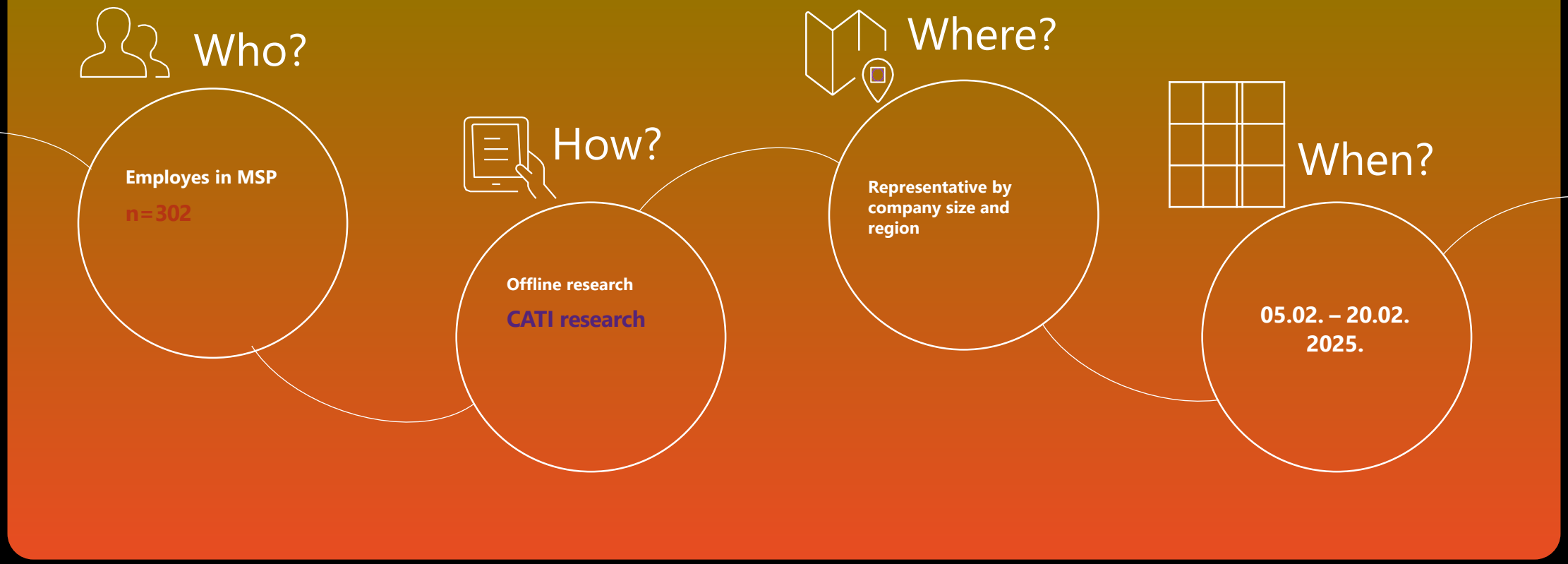
The goal of this research is to assess the level of awareness and application of cyber hygiene among employees in different types of enterprises. The study examines how familiar employees are with the concept of cyber hygiene and which security practices they apply in their daily work. It also analyzes the relationship between company size and type and the level of cyber hygiene, as well as the challenges organizations face in improving cybersecurity. Special focus is placed on evaluating internal policies and procedures related to incident reporting and the use of security tools. The research further explores the level of investment in cybersecurity, obstacles to its improvement, and the readiness of companies to respond to cyber incidents. Through the analysis of the results, the aim is to identify key weaknesses and propose concrete measures to enhance cyber hygiene within organizations. The ultimate goal is to raise cybersecurity awareness and strengthen the protection of both business and personal data.

Survey goal

Note

The percentages presented in this document may not always total 100 due to: rounding effects and the design of the questionnaire with multiple-response options (for some questions, respondents were able to select more than one answer – in such cases, the total may exceed 100).

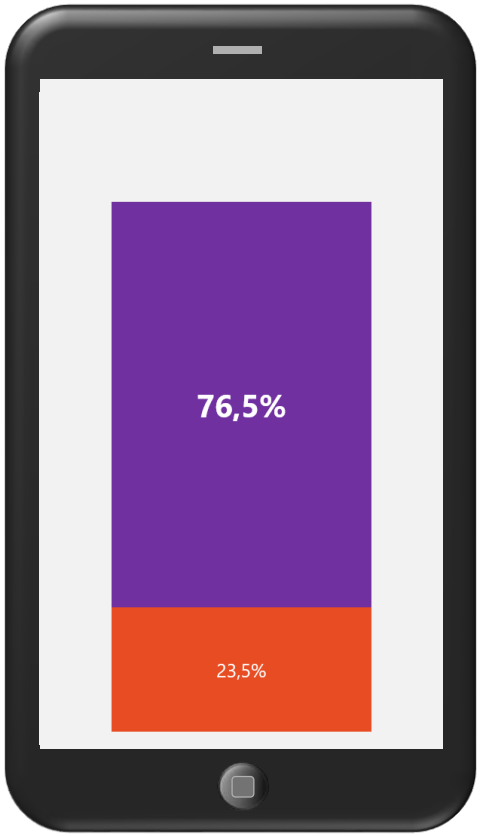
STARSUP



Methodology and sample


Awareness of cyber hygiene measures in companies
STARSUP

Are you familiar with the term "cyber hygiene" in the context of a business environment?



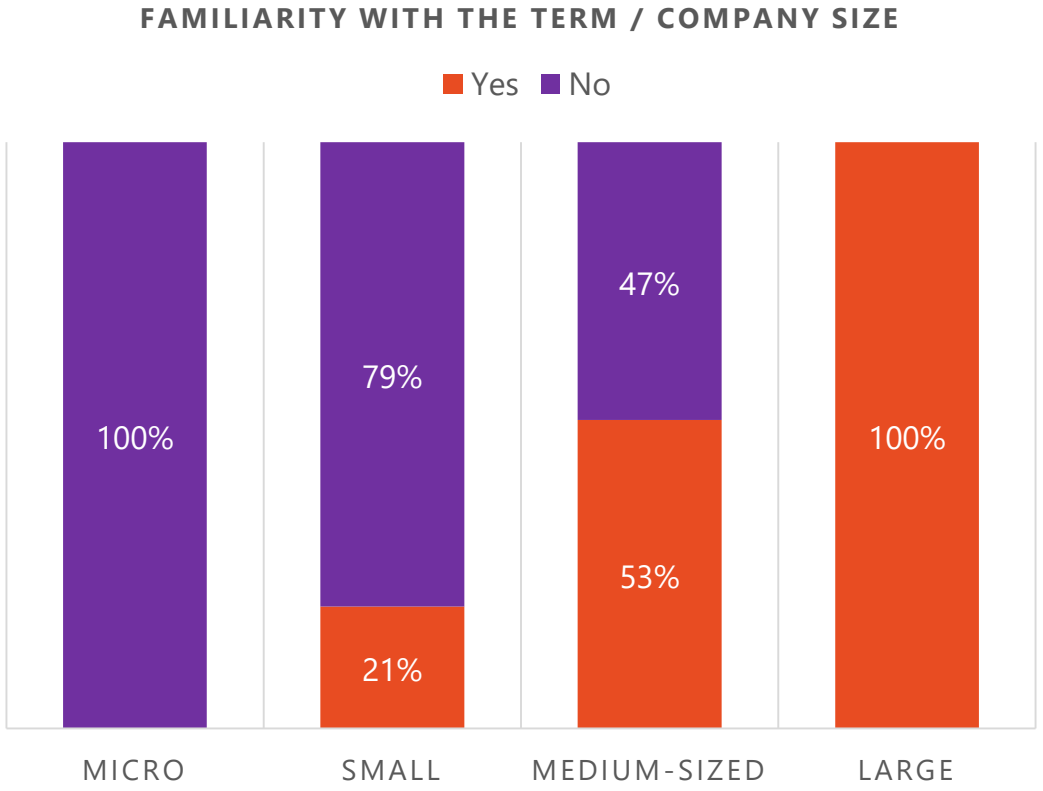
76.5% of respondents stated that they **are not familiar with the concept of cyber hygiene.**

These findings indicate a serious lack of awareness and understanding of basic digital security principles. They may also have significant consequences for the security of both personal and business data.

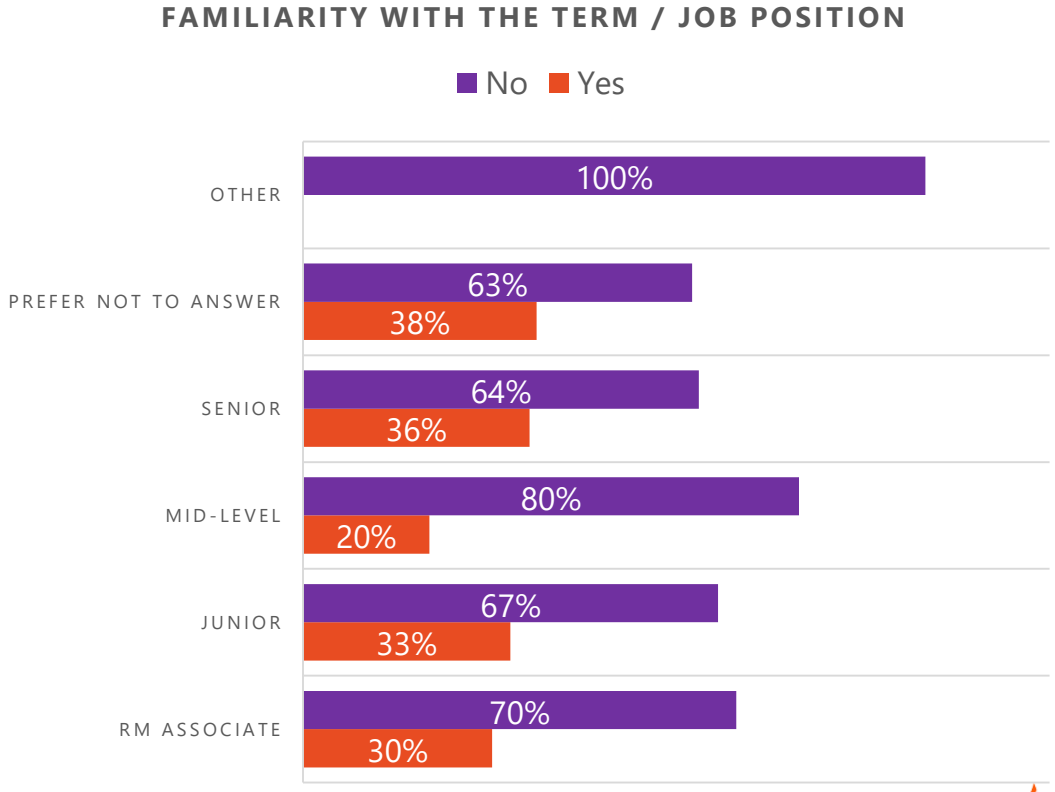
N=303

The results show significant differences in familiarity with the term “cyber hygiene” depending on company size. However, a higher job position is not necessarily associated with greater knowledge of cyber hygiene, although certain variations do exist among the groups.

p-value of 0,000, **p < 0,05**, we can conclude that there is a statistically significant association between company size and the level of cyber hygiene awareness. The same conclusion applies when comparing the level of cyber hygiene awareness with company revenue.



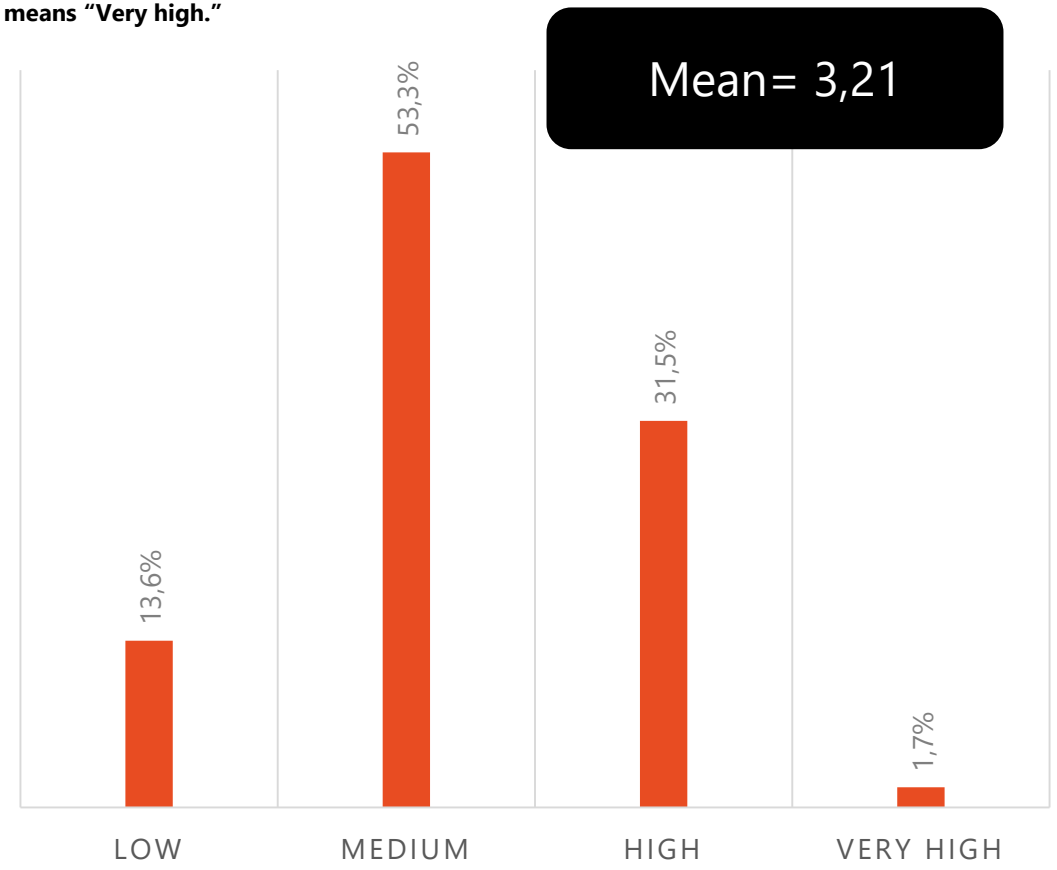
p-value of 0,369787, **p > 0,05**, we can conclude that there is no statistically significant association between an employee’s job position or experience and their level of cyber hygiene awareness.



STARSUP

Based on the presented data, the level of cyber hygiene can be assessed as moderate, given that the largest share of respondents (53.3%) falls into this category. Here are some key observations:

After the previous explanation, how would you rate the **overall level of understanding of cyber hygiene within your company's business processes**?
We will use a scale from 1 to 5, where **1 means "Very low"** and **5 means "Very high."**



Positive aspects:

- More than half of respondents practice a **moderate** level of cyber hygiene, indicating a certain level of awareness and basic security practices.
- Only **1.7%** of respondents demonstrate a **very high** level of cyber hygiene, which—although a small percentage—shows that there is a group consistently applying advanced security measures.

Concerning aspects:

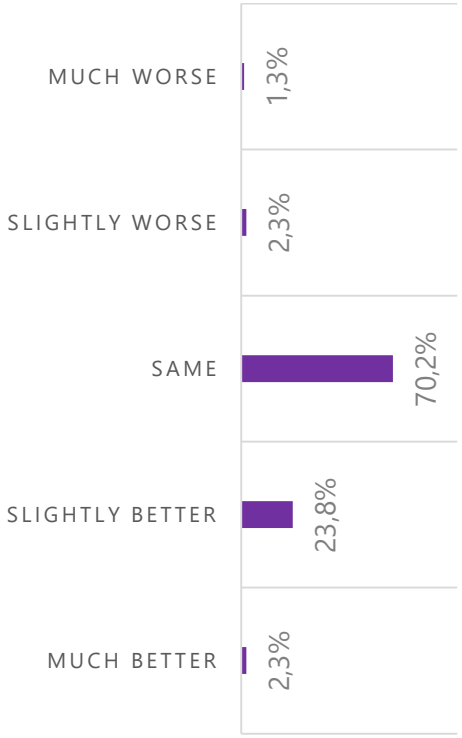
- **13.6%** of respondents have a **low** level of cyber hygiene, which may represent a significant security risk for both personal and business data.
- The small percentage in the **very high** category suggests that there is room for improvement in adopting advanced practices such as two-factor authentication, regular software updates, and awareness of phishing attacks.

STARSUP

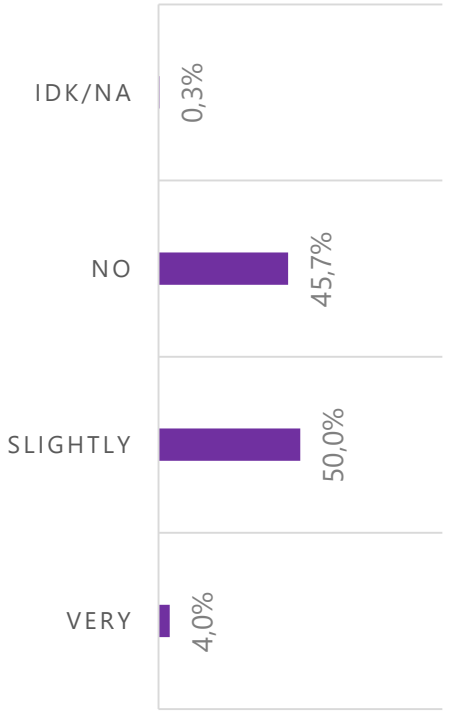
The research results indicate a moderate recognition of the importance of cyber hygiene, but also reveal serious shortcomings in the implementation of cybersecurity measures and incident response. This points to the need for more intensive training, increased awareness of the importance of cyber hygiene, and the improvement of existing security policies in order to reduce the risk of potential cyber incidents.

How do you assess the importance of cyber hygiene in the business environment?

How would you rate your company's cyber hygiene skills compared to others?



Do you believe that the cybersecurity measures and incident response capabilities in your company are at a satisfactory level?



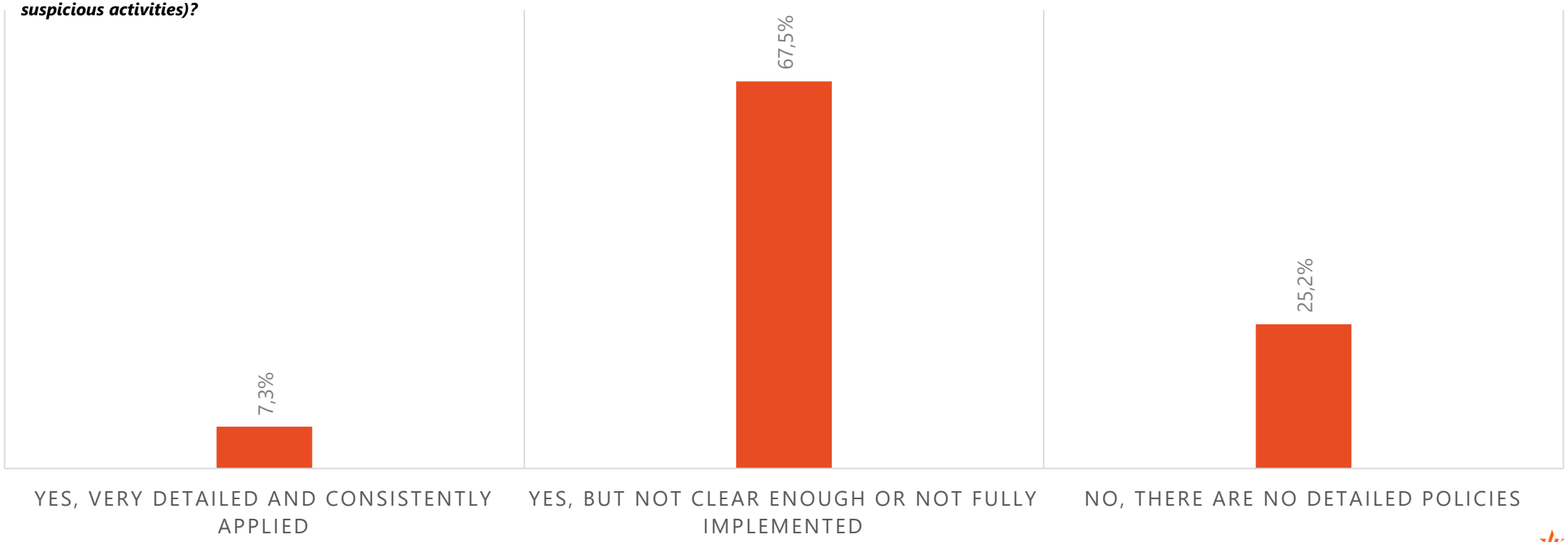
N=302

Most respondents (**72.8%**) consider the importance of cyber hygiene to be moderate, while only **21.1%** view this area as highly or very highly important. This perception correlates with the assessment of cyber hygiene skills compared to other small and medium-sized enterprises (SMEs), where **70.2%** of respondents believe their company is on the same level as the competition. However, only **26.1%** believe their skills are somewhat or significantly better, indicating a lack of competitive advantage in the domain of cybersecurity.It is concerning that **45.7%** of respondents believe that cybersecurity measures and incident response capabilities are not satisfactory, while **50%** rated them as somewhat satisfactory. This suggests that a significant number of organizations lack adequate mechanisms for protection against cyber threats and do not have sufficiently developed capacities to respond in the event of an attack.

STARSUP

Most companies (67.5%) have cyber hygiene policies, but these policies are either unclear or not applied consistently, which increases the risk of security breaches. Only 7.3% of companies have detailed and actively implemented policies, while 25.2% have no defined guidelines at all. These findings highlight an urgent need for clearer rules, consistent enforcement, and employee training.

Does your company have clearly established policies related to cyber hygiene (e.g., rules on password use, software updates, and reporting suspicious activities)?

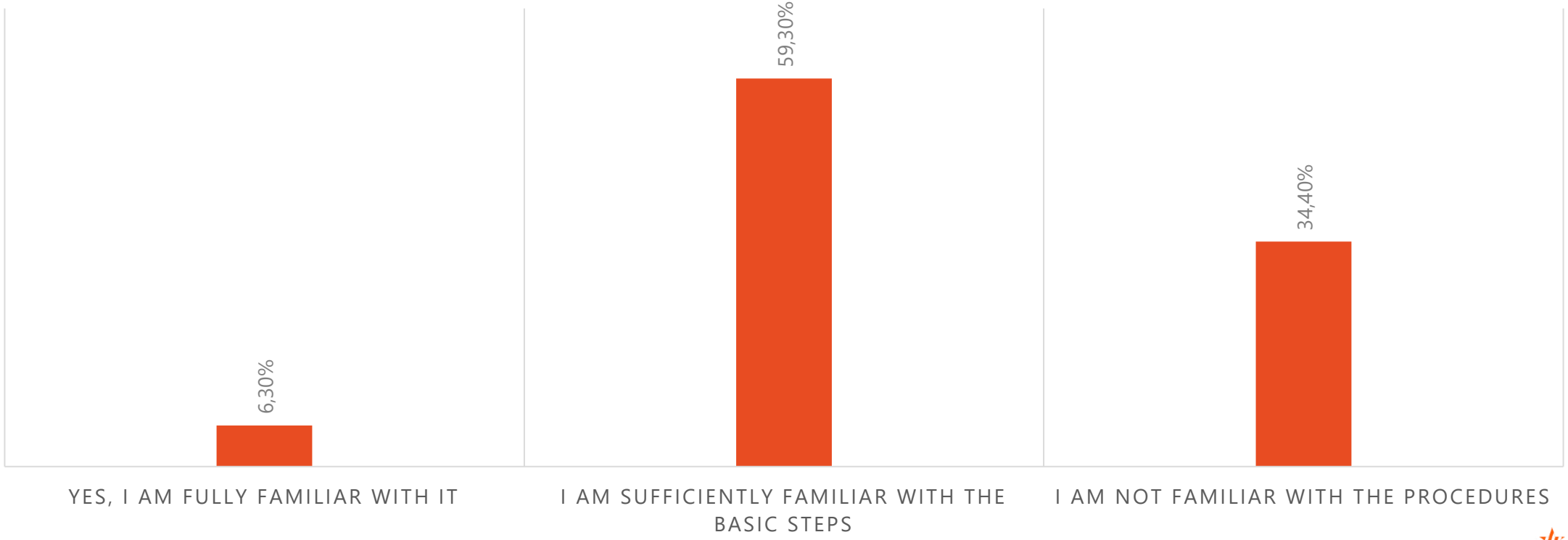


N=302

STARSUP

The results show that only 6.3% of respondents are fully familiar with the procedures for reporting suspicious cyber incidents, while 59.3% know the basic steps. It is concerning that as many as 34.4% of respondents are not familiar with the reporting process, indicating a serious lack of communication and training in this area.

Are you familiar with the process for reporting suspicious cyber incidents in your company (e.g., phishing emails, suspicious links)?

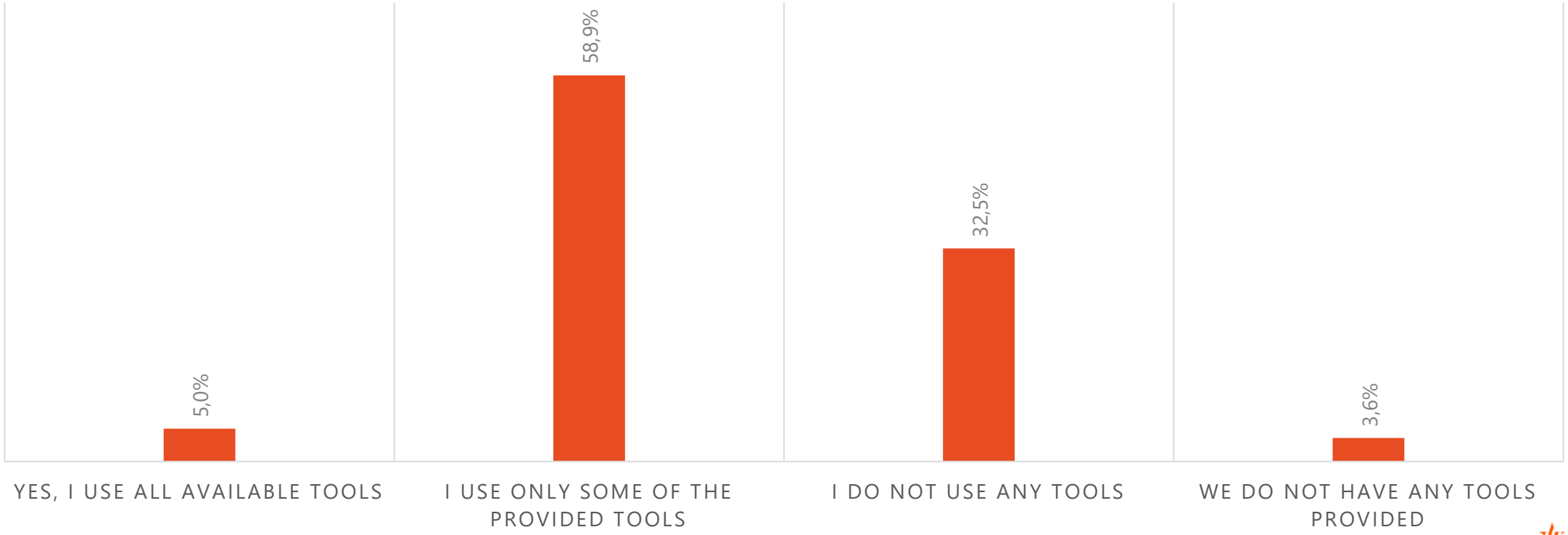


N=302

STARSUP

The results show that only 5% of respondents use all available cybersecurity tools, while 58.9% use only some of them. It is concerning that 32.5% do not use any tools, and 3.6% report that their company does not provide any security tools at all.

Do you use the cybersecurity tools provided by your company?



N=302

STARSUP

Although many companies have implemented basic cybersecurity tools, their use is not consistent, and a significant number of employees are not aware of the solutions available to them.

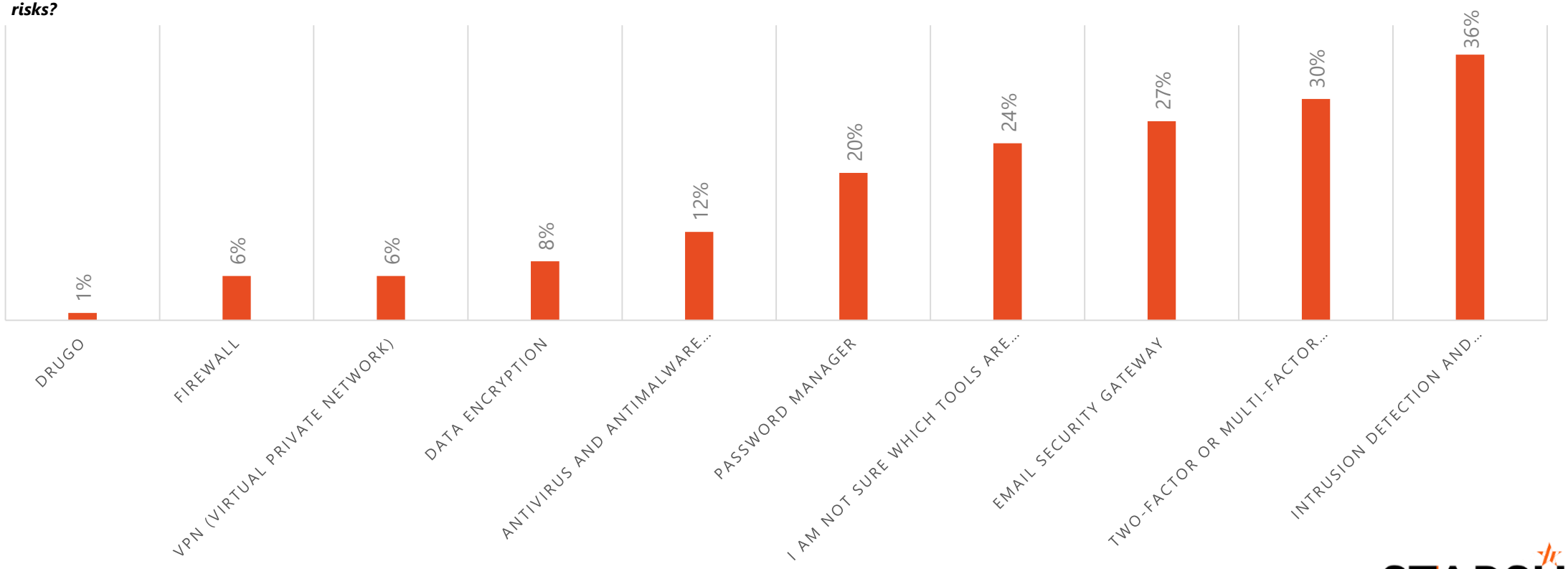
There is a need to strengthen training efforts and promote the active use of these tools in order to reduce exposure to cyber threats.

STARSUP

Intrusion Detection and Prevention Systems (IDS/IPS) – 36%,Two-factor or multi-factor authentication (2FA/MFA) – 30%,Email security gateway software – 27%,are the most commonly used tools.

However, 24% of respondents are not sure which tools are being used, indicating insufficient employee training regarding available security solutions. It is also important to note that key tools such as password management (20%), antivirus software (12%), and data encryption (8%) are not widely used, which may pose a serious security risk.

Which technological tools and solutions does your company use to manage cybersecurity risks?

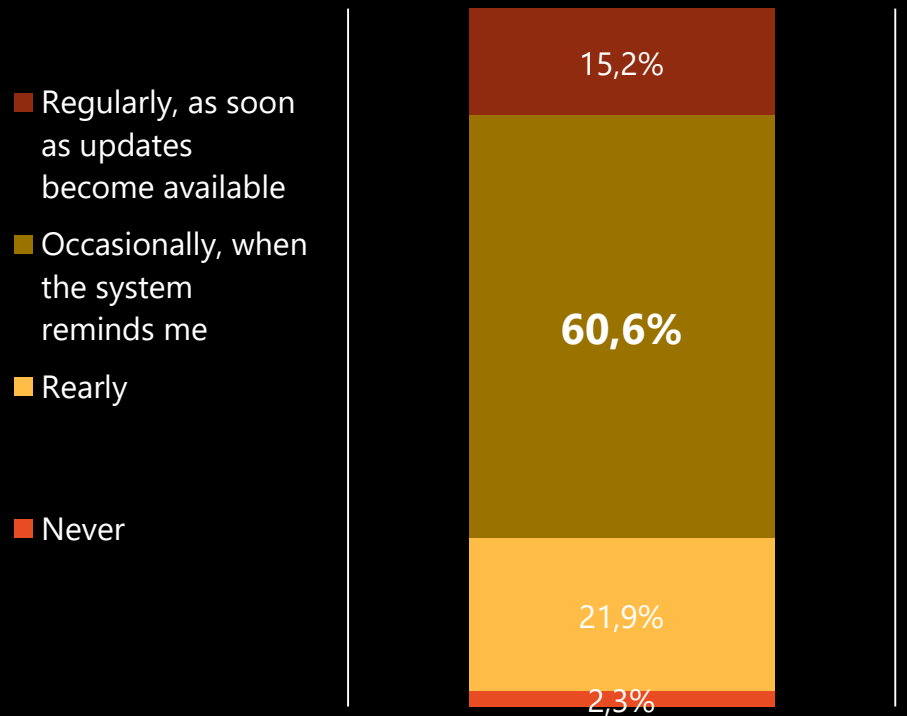


N=193

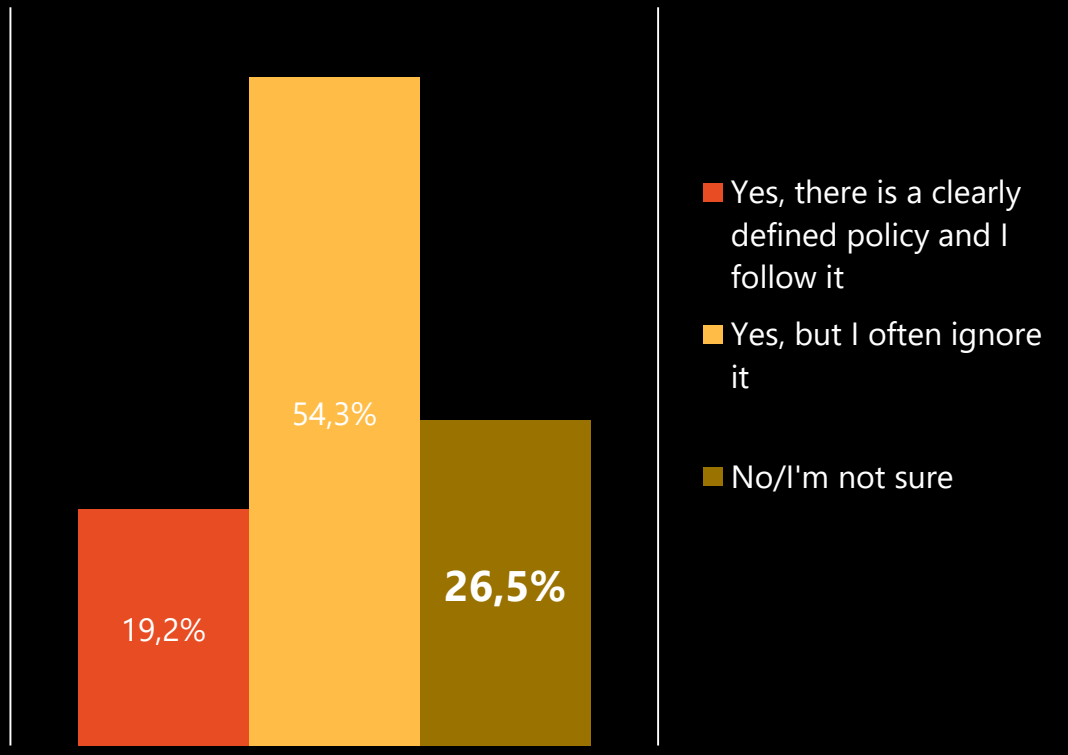
STARSUP

Most users update their work devices and applications only when the system reminds them (60.6%), while 21.9% update them rarely and 2.3% never update them at all, which increases the risk of cyberattacks due to outdated software. Additionally, although 54.3% of employees have a policy requiring regular password changes, they often ignore it, while 26.5% are unsure whether such a policy even exists. This highlights the need for stricter rules and employee training to increase accountability in maintaining cybersecurity.

How often do you update the work devices and applications you use?



Do you have an obligation to regularly change the passwords for your work accounts according to your company's policies?

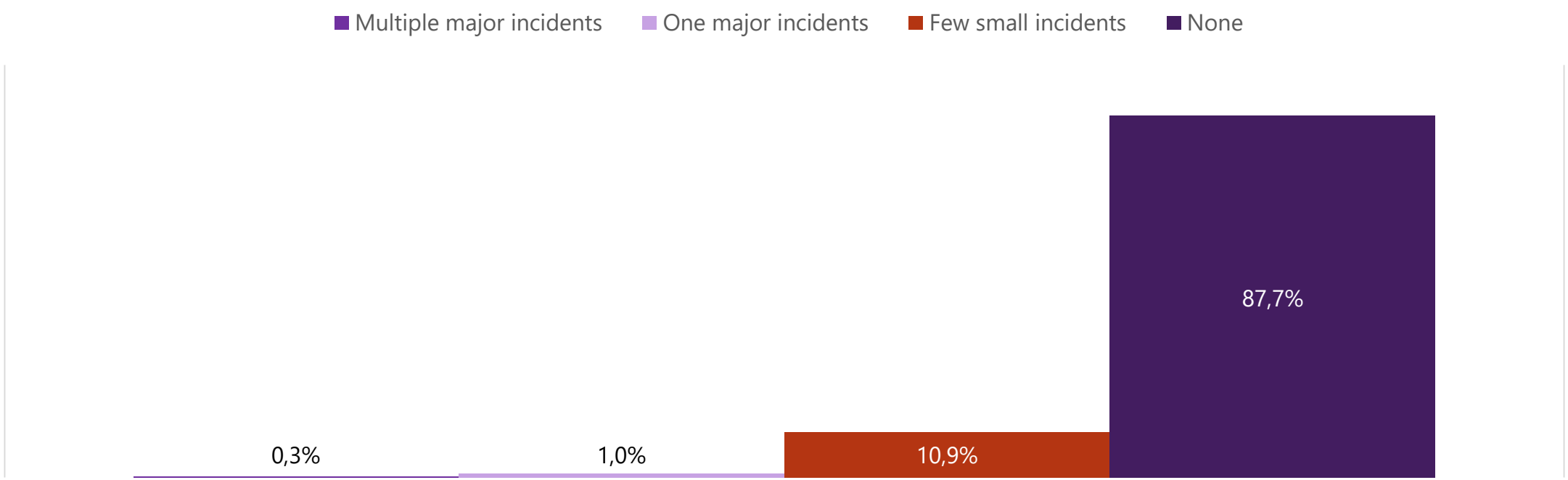


N=302

STARSUP

Most companies (87.7%) did not report any cyber incidents in the past year, while 10.9% experienced several minor incidents, and only 1.3% reported one or more major attacks. Although these figures may appear encouraging, it is possible that some companies were not even aware they had been targeted or did not properly report incidents. The absence of reported attacks does not necessarily indicate a high level of cybersecurity; rather, it may point to a lack of systems for threat detection and incident reporting.

How many cybersecurity-related incidents, if any, has your company experienced in the past year?

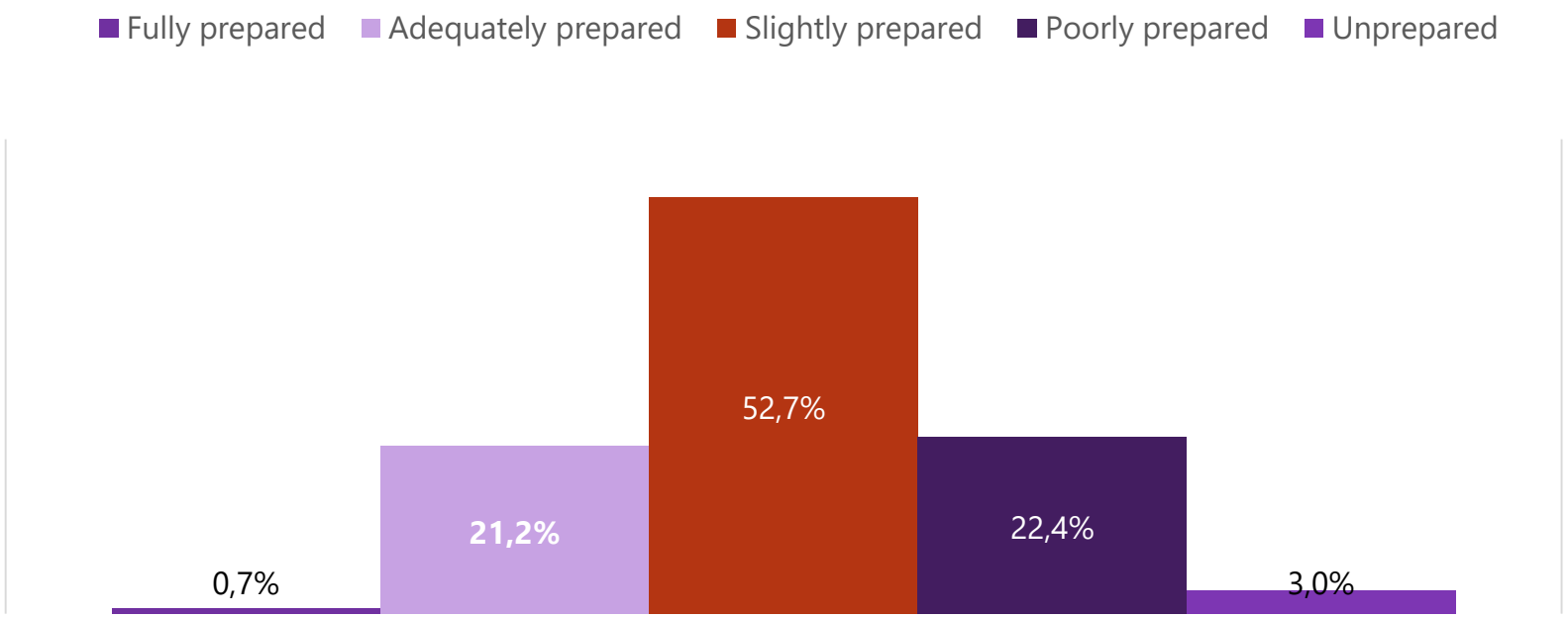


N=302

STARSUP

The data indicates substantial room for improvement through strengthening security policies, providing employee training, and implementing effective incident response plans. Although most companies have not experienced major incidents, their insufficient preparedness may become a critical factor in the event of a serious cyberattack.

Regardless of whether your company has experienced an incident or not, in your opinion, how prepared is your company to respond to cybersecurity-related incidents?



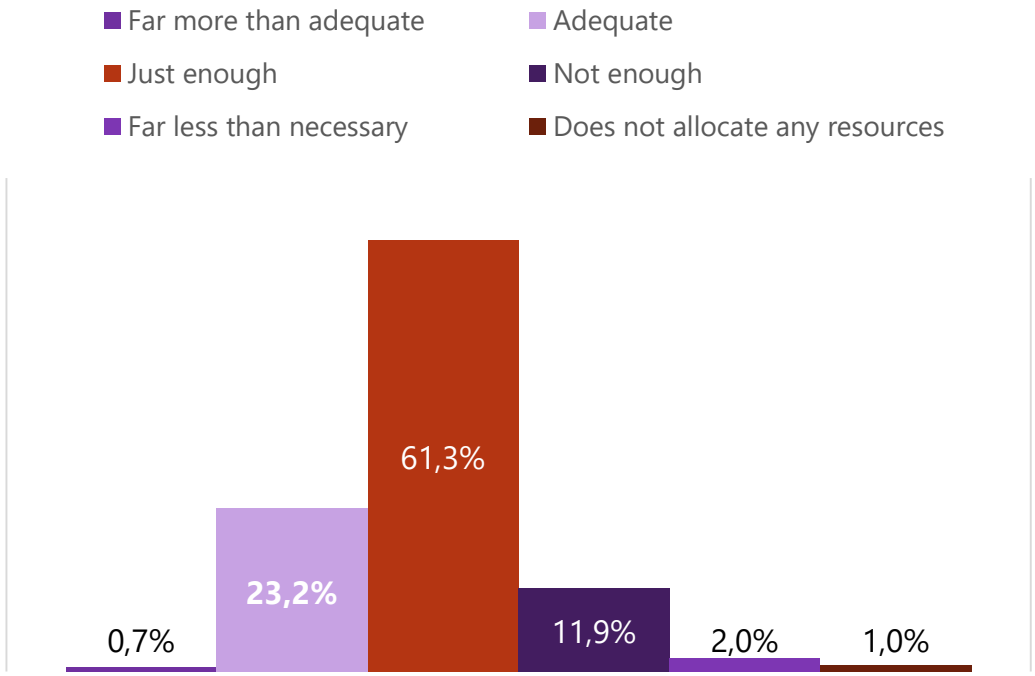
N=302

Most respondents believe that their company is only somewhat prepared to respond to cyber incidents (52.7%), while 22.4% rate their preparedness as poor and 3% as complete lack of readiness. Only 0.7% of companies consider themselves fully prepared, while 21.2% are adequately prepared.

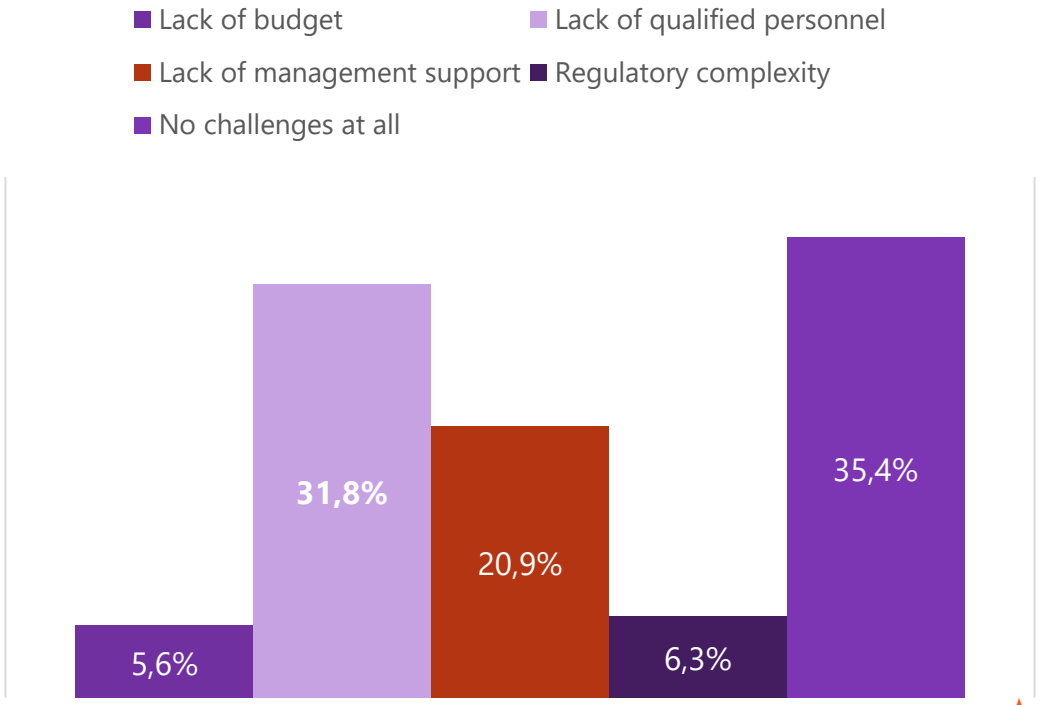
STARSUP

Most companies (61.3%) allocate only basic resources to cybersecurity, while 13.9% invest insufficiently or far less than required. The key challenges in improving cyber hygiene include a lack of qualified personnel (31.8%), insufficient management support (20.9%), and regulatory complexity (6.3%). Although 35.4% of companies report no challenges, the data suggests that many organizations lack adequate expertise and internal support to enhance their security posture.

Does your company allocate adequate resources (such as budget and personnel) for cybersecurity??



What are the primary challenges and obstacles your company faces in improving cyber hygiene?

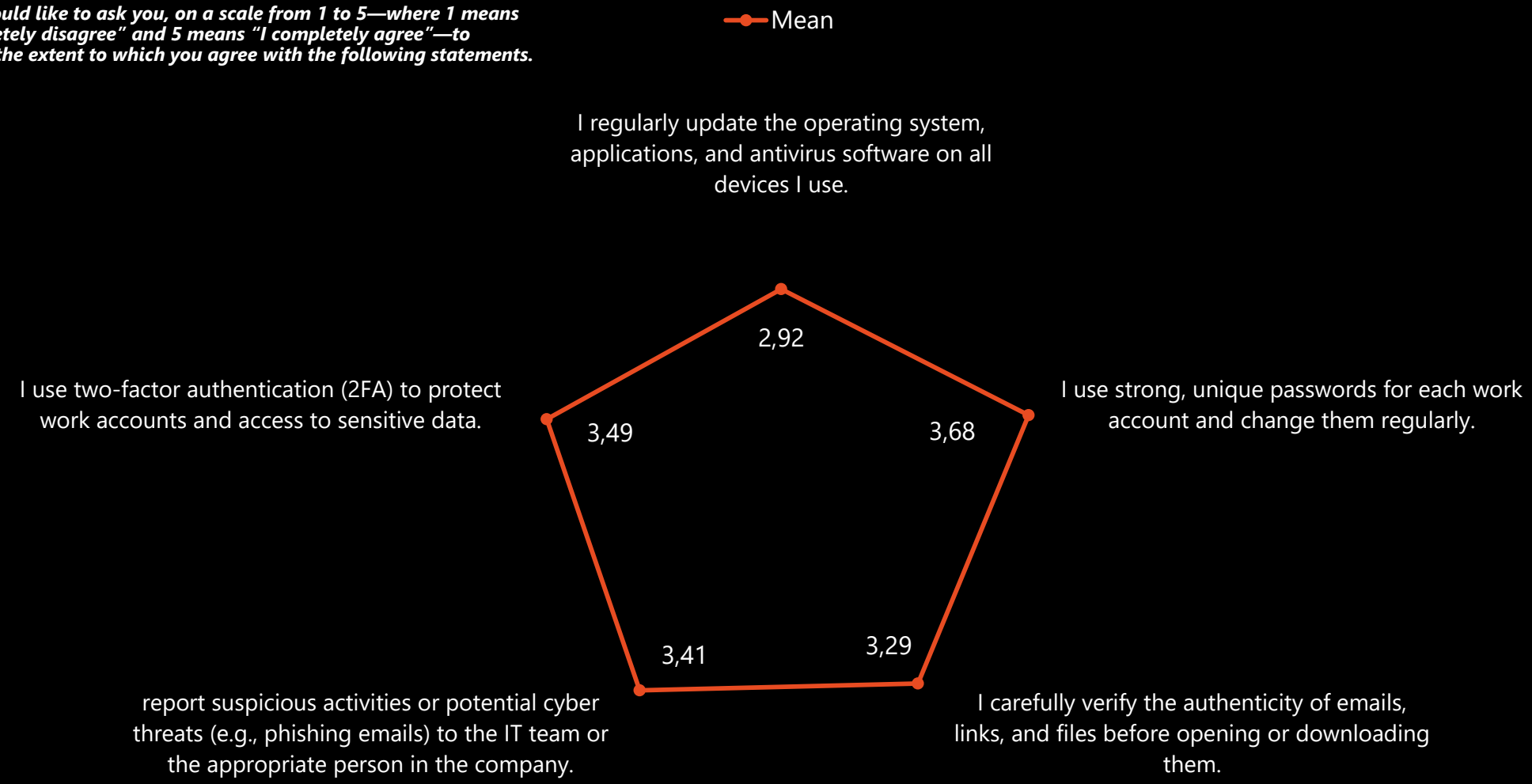


N=302

STARSUP

Employees most consistently adhere to the rules on using strong and unique passwords (average score 3.68) and two-factor authentication (2FA) (3.49), which is a positive indicator of awareness regarding account protection. Reporting suspicious activities (3.41) and verifying the authenticity of emails and links (3.29) are at a solid level, but still require improvement. The weakest area is the regular updating of operating systems, applications, and antivirus software (2.92), which represents a significant security risk.

Now I would like to ask you, on a scale from 1 to 5—where 1 means "I completely disagree" and 5 means "I completely agree"—to indicate the extent to which you agree with the following statements.



N=302

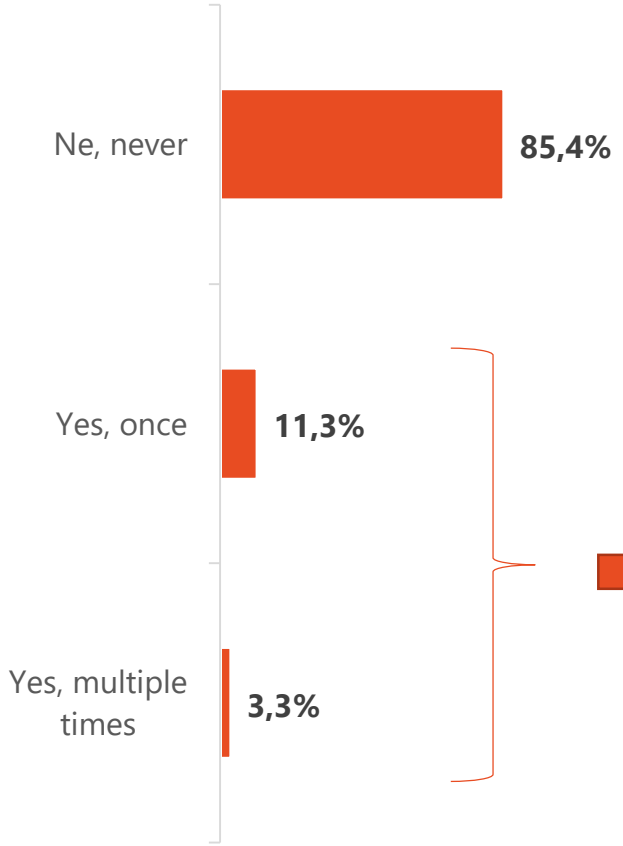
STARSUP

Training and need for training

STARSUP

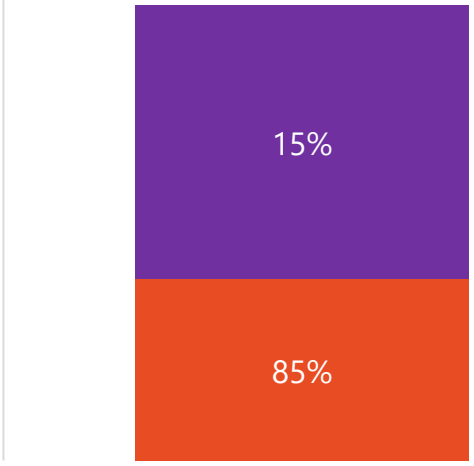
The results show that as many as 85.4% of employees have never undergone cybersecurity training, which represents a serious risk for companies. Among those who have completed some form of training, 85% consider it useful but believe there is room for improvement, while 15% feel it is not sufficiently practical. Interestingly, 83.4% of respondents do not consider training necessary, which may indicate low awareness of risks, a lack of interest in this topic, or a belief that solutions lie primarily in technical improvements rather than employee education.

Have you ever attended cybersecurity training within your company?



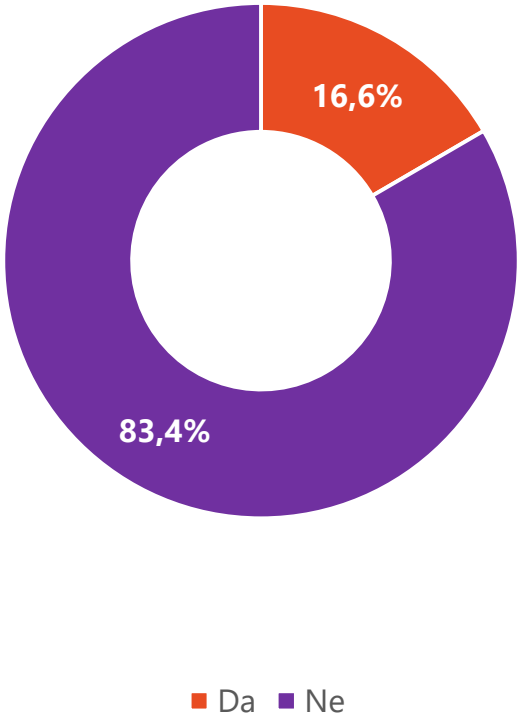
N=302

How would you rate the quality of the cybersecurity training your company organizes or has organized?



N=44

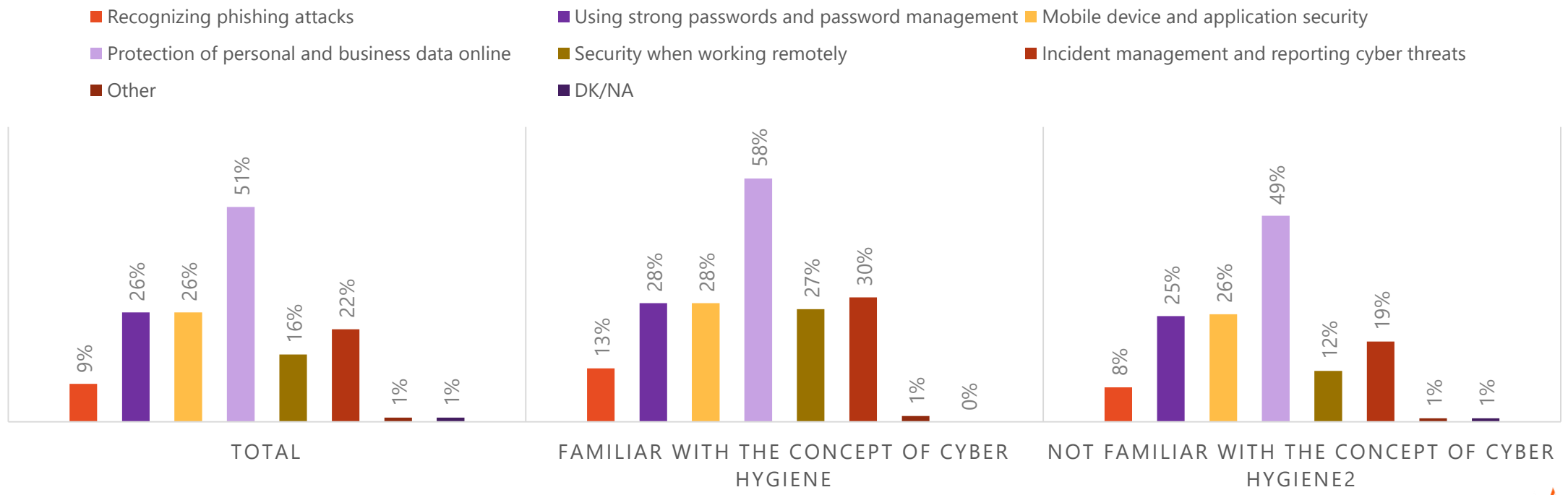
Do you believe that companies (and employees) similar to yours need cybersecurity training?



STARSUP

Individuals familiar with the concept of cyber hygiene demonstrate greater awareness of advanced security practices, particularly regarding remote work (27% vs. 12%) and incident management (30% vs. 19%). The protection of personal and business data is the most important topic for the majority of respondents (51%), with interest being higher among those who are familiar with cyber hygiene (58% vs. 49%). However, training on recognizing phishing attacks remains low even among the better-informed group (13%), indicating a clear need for additional education.

Which topics do you consider most important for cybersecurity training?

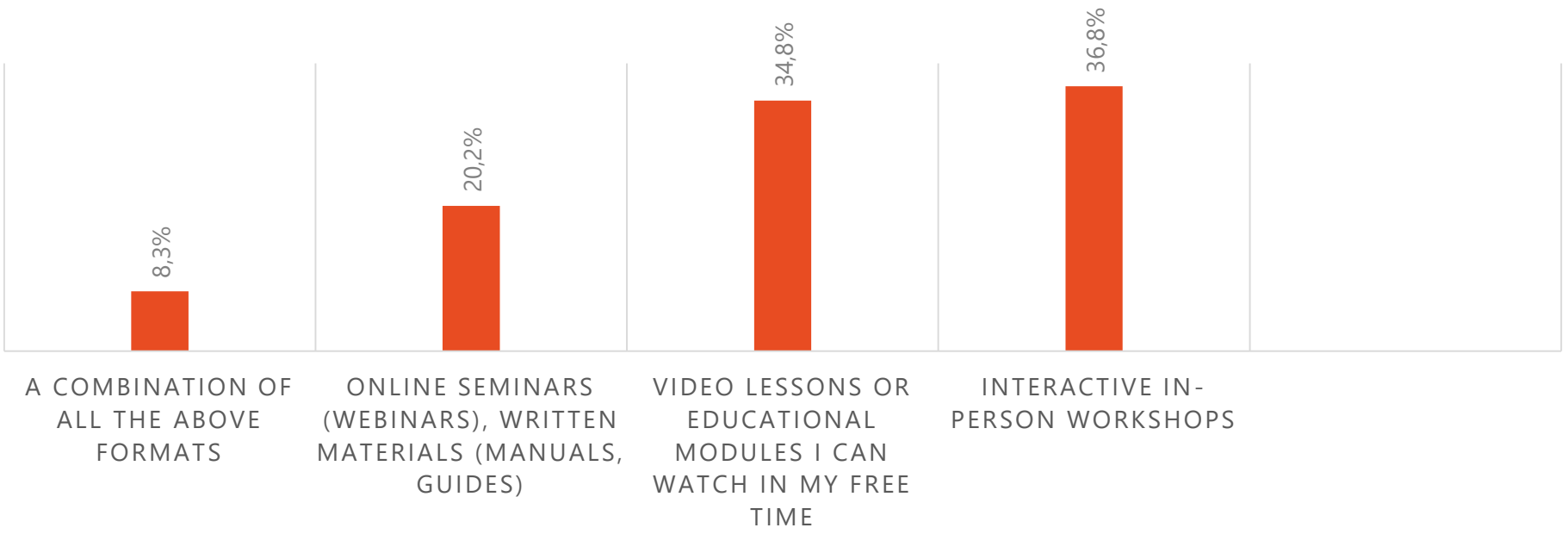


N=302

STARSUP

The most preferred training format is interactive in-person workshops (36.8%), indicating that employees value direct communication and hands-on learning. Video lessons and educational modules that can be followed in one's free time are the second most popular option (34.8%), reflecting a need for flexible learning. Webinars and written materials are less favored (20.2%), while only 8.3% of respondents prefer a combination of all formats.

How would you prefer to attend cybersecurity training?



N=302

To ensure training is effective, companies should focus on **interactive in-person workshops and flexible online video modules**, allowing employees to learn in the way that suits them best..

STARSUP

The largest share of respondents (42.7%) wish to improve the protection of personal and business data, indicating a growing awareness of the importance of information security. A total of 41.4% did not provide an answer (DK/NO), which may suggest a lack of interest or uncertainty about what they should learn. Interest in device protection (7%), comprehensive knowledge (7%), and protection against cyberattacks (2%) is relatively low, highlighting the need for further awareness-raising about threats that go beyond data protection alone.

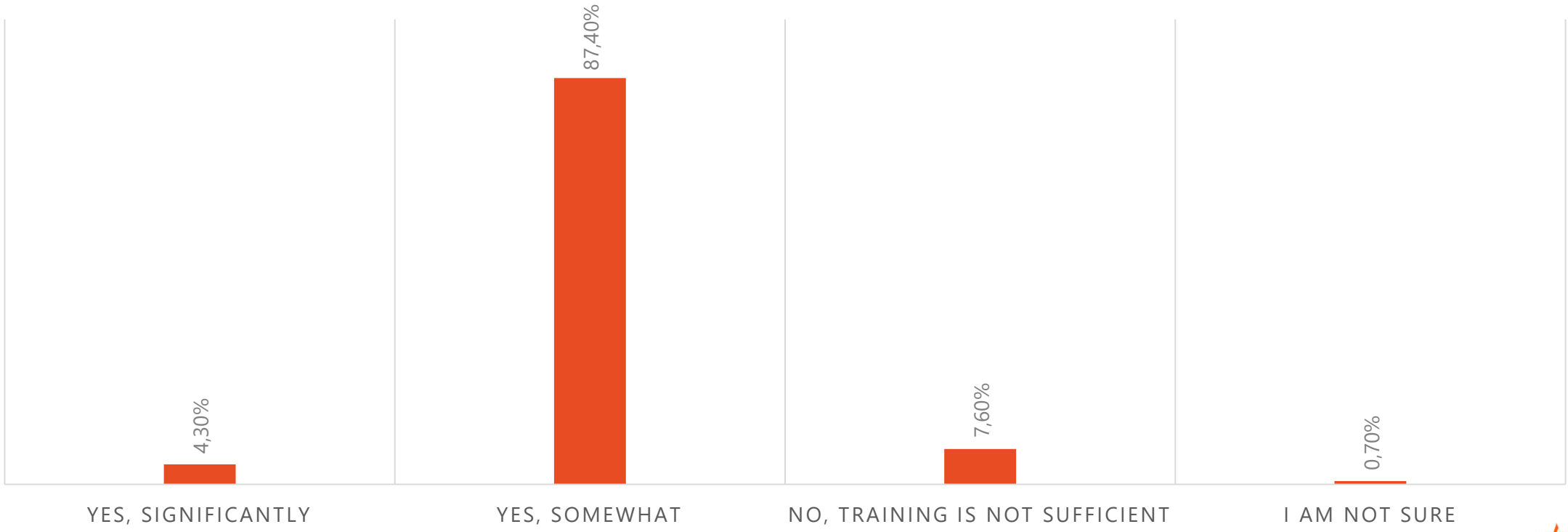
What would you like to learn or improve regarding cybersecurity?

N=302

STARSUP

The vast majority of respondents (87.4%) believe that additional training would somewhat help reduce the risk of cyber incidents, while 4.3% think the impact would be significant. On the other hand, 7.6% of respondents do not consider training sufficient, suggesting the need for additional measures such as technical security solutions and stricter policies. A very small number of respondents (0.7%) are unsure about the impact of training.

Do you believe that additional training would help reduce the risk of cyber incidents in your company?



N=302

STARSUP

Recommendations for improving cyber hygiene in companies

STARSUP

Based on the data analysis, the following measures are recommended to improve cyber hygiene and reduce the risk of cyber incidents:

1. Employee education and awareness-raising

- Organize **mandatory training sessions** on the basic principles of cyber hygiene, tailored to different employee levels.
- Focus on topics such as **recognizing phishing attacks, password management, data protection**, and the **secure use of work devices**.
- Implement **interactive in-person workshops** (36.8%) and **video lessons** (34.8%), as employees have shown the highest interest in these formats.
- Test employees through **simulated cyberattacks** to assess their readiness for real threats.

Based on the data analysis, the following measures are recommended to improve cyber hygiene and reduce the risk of cyber incidents:

2. Improvement of cybersecurity policies and procedures

- Define and **clearly communicate cyber hygiene policies**, including rules on passwords, incident reporting, and software updates.
- Make the **process of reporting cyber incidents simple and easily accessible** to encourage employees to report suspicious activities.
- Establish **mandatory guidelines for two-factor authentication** (2FA) and ensure its implementation for all key business accounts.
- Develop an **incident response plan** so the company has clear steps to follow in the event of a cyberattack.

Based on the data analysis, the following measures are recommended to improve cyber hygiene and reduce the risk of cyber incidents:

3.Technical improvements and better implementation of tools

- Ensure the **mandatory use of intrusion detection and prevention systems** (IDS/IPS) and email security software, as these are among the most frequent targets of attacks.
- Increase the **use of password managers and antivirus software**, given that only a small percentage of employees currently use them.
- Implement **automated and mandatory software updates** to reduce the risk associated with outdated systems.
- Make sure all **employees** are **aware of which cybersecurity tools are available to them**, as 24% are unsure which tools their company uses.

Based on the data analysis, the following measures are recommended to improve cyber hygiene and reduce the risk of cyber incidents:

4. Increasing the budget and resources for cybersecurity

- Companies need to recognize that **investing in cybersecurity** is not an expense, but a means of protecting business operations and data.
- Promote increased budget allocation for **hiring qualified cybersecurity personnel**, given that the lack of experts is one of the biggest challenges.
- Ensure **strong management support** so that cybersecurity becomes integrated into all business processes rather than remaining solely within the technical department.

Sample structure

ECONOMY

TYPE OF ENTERPRISE	
Micro enterprise	1,70%
Small enterprise	90,70%
Medium-sized enterprise	6,30%
Large enterprise	1,30%

REVENUE	
Over EUR 2,000,000 annually	0,70%
|EUR 500.001 – 2.000.000 annually	1,00%
EUR 100.001 – 500.000 annually	11,30%
Up to EUR 100.000 annually	79,80%
Prefer not to answer	7,30%

NUMBER OF EMPLOYEES	
Up to 10 employess	89,40%
21-50 employess	8,30%
51-250 employess	0,30%
Over 251 employess	2,00%

Average number of women in the company (Mean)	16,12
Average number of women in managerial positions (Mean)	1,32

INDUSTRY	
Other	1,7%
Energy	1,3%
Finance and insurance	1,7%
Construction	,7%
Information technology (IT)	,7%
Creative industries and media	1,7%
Agriculture and food industry	,7%
Manufacturing	2,0%
Transport and logistics	4,0%
Trade (wholesale/retail)	8,9%
Hospitality and tourism	76,8%

IT sector	
Yes	4,00%
No	96,00%

REGION	
Central	45,70%
Southern	38,50%
Northern	15,80%

RESPONDENTS

GENDER	
Male	70%
Female	30%

AGE	
Under 25	4%
26-40	41%
41-64	55%
65+	0%

EDUCATION LEVEL	
Student	1%
Three-year/Four-year secondary school	65%
College/University degree	33%
Master's/Doctorate	1%

EMPLOYMENT STATUS	
Part-time employee	3%
Employer / Self-employed	21%
Associate	2%
Full-time employee	74%

POSITION	
Associate position	19%
Junior / Entry-level position	3%
Mid-level position	72%
Senior	4%
Other	0%
Prefer not to answer	3%

STARSUP

We are...

Montenegrin company that has been operating in the field of market research and public opinion polls for more than 6 years. We have high local presence and proven capacity to deliver high quality research.

We use the latest tools and techniques to provide insights that will help you make faster and smarter business decisions.

We can help you gather, analyse and interpret the informations you need to make data-driven decisions and make your business grow.

We conduct market research and opinion polling both locally and for some of the largest companies in the world.

NEW INSIGHTS ARE IMPERATIVE OF THE FUTURE.