REPORT

Map of Cybersecurity SMEs in Poland: Diagnosis, Needs, Recommendations

Industry Overview, Key Growth Factors, and Recommendations for Building a Competence Community

As part of the project NATIONAL COORDINATION CENTER – POLAND (NCC-PL)
co-financed by the Digital Europe Programme

| June 2025

NCC-PL National Cybersecurity Coordination Centre Poland
Ministry of Digital Affairs Republic of Poland
Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

About report

Ministry of Digital Affairs
Republic of Poland

Dear Readers,

Small and medium-sized enterprises are the foundation of the Polish economy and a key element in the development of innovative solutions in the field of cybersecurity. Within these companies the future leaders of Polish cybersecurity are born, creating innovative technologies, building services and supporting digital resilience in both the private and public sectors. Their role in shaping the future of cybersecurity in Poland cannot be overestimated.

As part of the National Coordination Centre - Poland [NCC-PL] project, co-financed by the Digital Europe Program and implemented by National Coordination Center at the Ministry of Digital Affairs, a report Map of cybersecurity SMEs in Poland: diagnosis, needs, recommendations was developed, presenting a multifaceted picture of this sector. The conclusions presented in the report are highly reliable and of great analytical value as they are based on a very large sample covering a significant part of the cybersecurity industry, and the recommendations were developed with the participation of representatives of the cybersecurity ecosystem.

I am convinced that this study on the potential and needs of SMEs from cybersecurity sector is not only the knowledge but also a useful tool for creating effective public policy supporting cybersecurity industry in Poland, based not on intuition but on reliable data and the direct voice (not always favorable) of small and medium-sized enterprises, which must be heard and whose needs must be addressed in a realistic manner.

I hope that reading this document will inspire you to your own reflections and will encourge entities with the motivation and potential - to join the efforts to develop cybersecurity in Poland and Europe through a Competence community that supports the goals and tasks of European Cybersecurity Competence Center and of the National Coordination Center. I invite you to cooperate and contact NCC-PL, all information can be found at www.gov.pl/web/cyber-nccpl.

Finally, I would like to express my gratitude to all the experts and representatives of small and medium-sized enterprises who selflessly donated their time to take part in the study. Without your commitment, the Map of cybersecurity SMEs in Poland would not have been possible.

Thank you!

Paweł Olszewski

Secretary of State at the Ministry of Digital Affairs

Dear Readers,

In this report, we have focused in particular on presenting a comprehensive picture of the SME sector within the cybersecurity industry in Poland. We examined how Polish small and medium-sized enterprises structure their operational and HR models, as well as how they approach internationalization, access to financing, and the implementation of EU regulations. Unfortunately, as many as 77% of the surveyed companies admitted they have never benefited from any form of public support to develop their cybersecurity operations. One in three companies declared an interest in international expansion, but in practice, these efforts are often limited to isolated projects or remain at the planning stage.

What is the current state of the industry? How can we support SME development and strengthen the national potential of the cybersecurity sector? These are the central questions addressed in this report.

I wish you an insightful read and fruitful reflections, with the hope that the findings will contribute to the growth and more effective development of the sector.

Emilian Kołodziej

CEO IBC Advisory S.A.

Table of Contents

About report....2
Table of Contents....4
Introduction....5
Key finding and recommendations....8
1. Key Findings....10
2. Recommendations....11
Overview of the Polish cybersecurity industry....14
1.1. Mapping the Cybersecurity Sector....15
1.2. Sector Ecosystem Analysis....18
1.3. Overview of Small and Medium Enterprises in Poland's Cybersecurity Sector....20
1.4. Business models....28
Strengths and Prospects of Domestic Cybersecurity SMEs....31
2.1. Human Resources and Competencies (based on ECSF)....32
2.2. Technological and Infrastructural Potential....40
2.3. Certification....48
2.4. Types of Funding....53
2.5. Internationalization of Companies....63
2.6. Analysis of Cooperative Links....66
Barriers and development needs of Polish SMEs in the cybersecurity sector....67
3.1. Growth Barriers - Financial, Organizational, Regulatory....68
3.2. Regulations of the Polish Cybersecurity Market....78
3.3. Expectations Toward the Institutional and Legislative Environment....83
Bibliography....91
List of Charts and Figures....93

Introduction

The aim of this study is to identify the potential, barriers, and development directions of the SME sector within the cybersecurity field in Poland. The report serves as a foundation for formulating recommendations for public administration and other stakeholders involved in building the national and European cybersecurity ecosystem. Special attention is given to identifying entities which—due to their resources, competencies, and business profiles—can be included in the so-called Competence Community, in accordance with Article 8 of Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021.

The Competent Community, developed by the National Cybersecurity Competence Centre (NCC-PL), is an initiative aimed at integrating entities with expertise and experience in the field of cybersecurity. Joining the Community enables entrepreneurs to gain access to specialized knowledge, innovative technologies, and opportunities to collaborate with key actors from the public, academic, and business sectors—both at the national and European levels.

Participation in the Community facilitates networking for companies, especially SMEs, provides access to information on available funding sources, and enhances their visibility in the cybersecurity market. Membership also fosters the exchange of experience, joint problem-solving within the industry, and better preparedness for implementing new regulations such as the NIS2 directive.

Through participation in this initiative, companies will receive tangible support in developing workforce competencies, implementing innovative products and services, and strengthening their competitive position in the European market.

Scope and Objectives of the Study

The study was cross-sectional in nature and encompassed both a structural analysis of the national cybersecurity SME market and a diagnosis of needs and constraints at the operational, strategic, and systemic levels. The general objectives of the study included:

1. Developing a map of the cybersecurity industry in the SME segment, taking into account specialization, territorial reach, type of activity, and operational scale.
2. Determining short- and medium-term development prospects for the sector.
3. Diagnosing growth barriers—including financial, organizational, and regulatory—that hinder expansion and innovation.
4. Developing recommendations for public institutions to improve business conditions and enhance the competitiveness of domestic enterprises.
5. Identifying high-potential entities that could actively participate in the *Competence Community* initiatives.

The specific objectives included, among others: creating appropriate research tools (questionnaires, interview scenarios), developing criteria for sector inclusion, analyzing certification levels, international experience, and firms' readiness to participate in acceleration and cooperation projects.

Methodology

The study employed an innovative approach using a mixed-methods design that combined both quantitative and qualitative components:

- **Desk Research** – Analysis of source documents, statistical data, industry reports, and legal regulations. This served as the starting point for understanding the market and regulatory context. As part of this component, based on data from over 400 companies, a **Map of Small and Medium-Sized Enterprises in the Cybersecurity Sector** was created.
- **CAWI/CATI Survey** – A quantitative survey conducted among 197 cybersecurity sector enterprises of various types, locations, and sizes.
- **In-Depth Interviews (IDI)** – 20 individual interviews with company representatives, which enabled deeper diagnosis and insight into subtle dependencies influencing strategic decision-making.
- **Expert panels** – As part of the study, two expert panels were conducted: one at the beginning of the research process during the development of research tools, and another at the end during the formulation of recommendations. The panels included representatives of Polish SMEs operating in the cybersecurity sector, including CEOs and directors of these companies.

This approach allowed for data triangulation and enabled both a quantitative snapshot of the sector and an understanding of decision-makers' perspectives, institutional barriers, and company concerns related to expansion, certification, and international cooperation.

Structure of the Report

The report is divided into three main sections, covering both contextual analysis and detailed empirical findings along with operational conclusions. Each section includes subsections focusing on key aspects of the functioning of the national SME cybersecurity sector.

1. Characteristics of the Polish Cybersecurity Sector (Desk Research)

The first section presents a synthetic analysis of the cybersecurity landscape in Poland. It includes:

- Terminological definitions and clarifications,
- Analysis of the market's size and structure (including value and growth dynamics),
- Identification of key ecosystem institutions (e.g., NASK, CSIRTs, Ministry of Digital Affairs),
- Overview of applicable national and EU acts affecting business operations (e.g., NIS2, DORA, GDPR, CRA),
- Identification of factors stimulating demand for cybersecurity products and services,
- Overview of available financing options and internationalization directions.

This section provides the conceptual foundation and context for interpreting data collected through the study.

The description of the sector is based on collected research data from 417 entities identified through mapping, which meet the criteria of Polish SMEs in the cybersecurity sector according to the adopted definition and methodology, as well as from 201 entities surveyed in detail through CAWI/CATI/IDI research.

2. Potential of Domestic SMEs in Cybersecurity

The second section presents an analysis of SME potential in terms of resources, technology, workforce, and organization. It focuses on:

- Employment structure and competences (based on ECSF – European Cybersecurity Skills Framework),
- Technical infrastructure and technology use,
- Possessed certifications, patents, and international experience,
- Financing models and investments in innovation.

This part assesses the extent to which enterprises are prepared for growth and participation in the European cybersecurity ecosystem.

3. Sectoral Barriers and Development Needs

The third section presents findings from the analysis of the main barriers and constraints hindering the development of cybersecurity SMEs. Based on qualitative (IDI) and quantitative (CAWI/CATI) data, it addresses:

- Financial, regulatory, and organizational obstacles,
- Entrepreneurs' expectations regarding institutional environment,
- Challenges in product certification and international expansion,
- The impact of NIS2 and CRA on operational activities.

This section provides detailed insights into the structural and systemic challenges that may require public policy intervention.

Key finding and recommendations

This report presents a comprehensive analysis of the cybersecurity sector in Poland, based on a commissioned study with particular emphasis on small and medium-sized enterprises (SMEs). The study combined desk research, in-depth interviews (IDIs) with representatives of cybersecurity companies, and a quantitative survey using CAWI/CATI methods. This mixed-methods approach made it possible to capture both structural conditions and the real operational and strategic challenges faced by the sector.

The SME cybersecurity market in Poland is highly diverse in terms of company size, business experience, capital origin, and scope of activity. The vast majority of surveyed companies were small enterprises (160 out of 197), most of which have been active for more than four years—many for over a decade. These businesses are predominantly domestically owned, with only a few being part of foreign corporate structures. The activity profile of SMEs in the sector is broad—many operate simultaneously in consulting, training, systems integration, penetration testing, and software development—indicating a high level of specialization and operational flexibility. The highest regional concentration of cybersecurity firms is found in the Mazowieckie Voivodeship, followed by Wielkopolskie, Śląskie, Małopolskie, and Dolnośląskie. Most companies are service providers or integrators, active in incident monitoring, identity and access management, compliance, and security testing. Despite the growing importance of cloud and OT (operational technology) security, traditional IT security areas—such as network and endpoint protection and vulnerability management—remain dominant.

The research portrays a dynamic and rapidly growing sector characterized by organizational flexibility but burdened by multiple developmental barriers. SMEs often rely on hybrid employment models and collaborate with external experts and academia. A critical issue is the shortage of highly qualified specialists, especially for cross-functional roles that combine technical, strategic, and commercial skills. This shortage is compounded by a lack of support competencies in areas like marketing, sales, and product management. Diversity—gender, age, or accessibility for people with disabilities—remains low, with most inclusion efforts being merely declarative.

The sector also faces limited access to funding—77% of surveyed companies have not used R&D grants, and 87% have not applied for international expansion support. Reasons cited include complex procedures, lack of knowledge about funding opportunities, and insufficient organizational capacity. Companies are also reluctant to pursue private investment, citing a lack of trust and unwillingness to give up equity.

The cybersecurity sector is under increasing regulatory pressure (NIS2, CRA, DORA), which simultaneously drives professionalization and imposes financial and organizational burdens—particularly on SMEs. At the same time, regulatory requirements in the field of cybersecurity contribute positively to the growing demand for cybersecurity products and services.

Despite these challenges, 42% of surveyed firms plan to invest in product and service development, including automation, SaaS offerings, and international expansion—especially into the EU, U.S., Middle East, and Asia. There is also demand for solutions in threat intelligence, AI/ML audits, and cloud security.

Most companies believe that development barriers can be overcome independently, but many also highlight the need for government support in regulatory, financial, and promotional areas. More than half of the respondents say public programs require improvement—commonly citing high certification costs, unclear procedures, and insufficient support. Businesses expect the state to act as a partner—not a controller—that ensures a level playing field with companies backed by foreign governments. Export support, promotion of domestic solutions, facilitation of public procurement access, and closer cooperation between academia and industry are seen as priorities. Firms call for long-term, multi-stage support programs instead of one-off grants, and better coordination between institutions. Awareness of AI's role in sector development is increasing, though some skepticism remains. Without a deliberate and proactive strategy, Poland risks losing its digital sovereignty and becoming a passive recipient of foreign technologies.

Based on the research findings, 16 detailed recommendations were developed, including simplification of funding systems, development of soft and sales skills, support for certification, promotion of acceleration programs, creation of science-business collaboration platforms, and professionalization of industry communication and advocacy. The report serves as a

starting point for strategic action, highlighting concrete areas of intervention and the need to establish long-term support mechanisms for SMEs that can serve as a foundation for a resilient, innovative, and competitive digital economy in Poland.

1. Key Findings

1. The cybersecurity sector in Poland is characterized by a flexible employment model - companies are increasingly shifting from full-time contracts to B2B and project-based cooperation, allowing them to respond more efficiently to changing market demands and optimize costs. Employment scale and form depend on the company's growth stage and project type - even larger organizations rely on external experts and cooperation with academic institutions. Stable, long-term teams are seen as a key asset, but companies report growing difficulties in hiring cross-functional specialists who combine technical, business, and communication skills. The main challenges concern hybrid roles such as architects, pre-sales leaders, and business development consultants. Although many firms claim gender neutrality, women remain underrepresented in technical teams, and individuals aged 65+ and persons with disabilities are nearly absent.

2. CAWI and IDI studies show that the main challenge for the Polish cybersecurity sector is the lack of developed threat prediction capabilities - companies tend to focus on reactive measures, while threat intelligence is often neglected. Cloud security and IAM systems are gaining importance, while the development of generative AI introduces risks related to code quality and the need for new audit standards. A shortage of specialists combining technical and business skills persists. Despite these challenges, nearly half of CAWI respondents plan to invest, mainly in R&D, new products, compliance with NIS2/DORA, and international expansion (EU, US, Middle East). IDI participants emphasized the public sector's role as an innovation buyer, though overregulation and bureaucracy remain major barriers. A striking 81% of companies have never participated in acceleration programs - indicating untapped potential. The sector is growing, but it needs investment in competencies, threat anticipation, and a more supportive regulatory environment.

3. The scope of operations among cybersecurity firms in Poland is diverse - most operate domestically, though many are expanding abroad. Main target regions include the EU, US, Southeast Asia, and the Middle East, where markets are receptive and less saturated. Expansion models include exports, partnerships, trade fairs, and subsidiaries. Despite strong ambitions, companies face obstacles such as high costs, public procurement barriers, cultural differences, and the difficulty of building business relationships. 64% of firms offer hybrid solutions (cloud/on-premise), and 39% use sales intermediaries. Many integrate products from other Polish firms, supporting the local ecosystem. Only 44% plan to certify their products, even though 72% declare knowledge of the process - this may limit competitiveness. Intellectual property protection is low - most firms do not hold patents or trademarks.

4. While the Polish cybersecurity sector is growing rapidly, its potential is constrained by numerous barriers. Companies face a lack of funding, skills shortages, and low market awareness of digital threats. Smaller firms struggle to acquire clients and compete with global brands that dominate public tenders and enjoy greater trust. Many organizations lack risk prediction tools, reducing the effectiveness of their preventive efforts.
   High certification costs, complex legislation (e.g., NIS2, CRA), and a lack of export support further hinder SME growth. Companies often lack sales and business development competencies, making scaling and internationalization more difficult. The public sector fails to fulfill its potential as a buyer and promoter of domestic solutions. There is an urgent need for regulatory simplification, financial support, and stronger industry collaboration to improve the international competitiveness of Polish firms.

2. Recommendations

1. Simplifying Access to Public Funding

Current procedures for accessing national and EU funding are overly complex, time-consuming, and poorly suited to the operational realities of SMEs. It is recommended to simplify application forms, shorten evaluation timelines, and implement dedicated support mechanisms (e.g. consultation points, mobile project advisors) to assist companies in preparing applications and budgeting projects. It is recommended to simplify and make more flexible the rules concerning own financial contribution in public funding programs, particularly those targeting the SME sector. Current requirements often exceed the organizational and financial capabilities of smaller companies, effectively discouraging them from applying for support. It is worth considering the introduction of mechanisms that adjust the required level of own contribution depending on the size of the enterprise, the level of project innovation, or the stage of company development. Such an approach would increase the accessibility of funding, enabling a broader group of companies to carry out investments in the field of cybersecurity and enhancing the effectiveness of public support instruments. These measures should particularly support R&D, internationalization, and compliance-driven implementations (e.g. NIS2, DORA, CRA).
Target institutions: Ministry of Funds and Regional Policy, Polish Agency for Enterprise Development (PARP), National Centre for Research and Development (NCBR), European Commission (for EU funds).

2. Development of Educational and Reskilling Programs

There is a lack of systemic initiatives to enhance technical and strategic skills in the sector. It is recommended to develop specialized educational paths at technical universities and general academic institutions (e.g. “Cybersecurity for Managers”, “Threat Intelligence”, “Cloud Security”), along with funding for reskilling courses for career changers. Collaboration with private companies should be a mandatory component of these programs.
Target institutions: Ministry of Education and Science, Higher Education Institutions, PARP, Employers / Tech Companies.

3. Support for SME Certification and Regulatory Compliance

The costs of obtaining certifications (e.g. ISO 27001, ENISA, Common Criteria, CE) are prohibitively high for small firms. It is recommended to establish financial support instruments such as certification grants or vouchers and to develop simplified compliance standards tailored to the capabilities of smaller entities. Advisory and audit support should also be provided.
Target institutions: PARP, Office of Technical Inspection, Ministry of Economic Development and Technology, Certification Bodies.

4. Building a Systemic DEI (Diversity, Equity, Inclusion) Policy

The sector should implement consistent DEI policies promoting the employment of women, older adults, and people with disabilities. This includes inclusive recruitment campaigns, workplace accessibility improvements, and anti-discrimination training for managers. Such practices could become eligibility criteria for selected public support programs.
Target institutions: Ministry of Family, Labour and Social Policy, Commissioner for Human Rights, PARP, DEI-focused NGOs.

5. Strengthening Science-Business Collaboration

There is a lack of sustainable mechanisms for knowledge transfer and joint R&D implementation. It is recommended to create competence centers, labs, and incubators at universities, where companies can test technologies in experimental environments. Universities should also serve as scientific partners in commercial and export-oriented projects.
Target institutions: Higher Education Institutions, NCBR, Ministry of Science and Higher Education, Private Companies.

6. Promotion and Expansion of Accelerator and Incubator Programs

Many firms do not engage with accelerators. It is recommended to provide financial and organizational support for dedicated cybersecurity accelerator programs. These should include mentoring, MVP testing, investor access, and international expansion pathways.
Target institutions: PARP, VC Funds / Accelerators.

7. Professionalization of Sales and Management Competencies

Technology firms often lack skills in sales, marketing, and business model development. It is recommended to launch a national training program in "Cyber Business Management" for tech founders and technical leads. Modules should cover strategy, client acquisition, tech storytelling, and company valuation.
Target institutions: PARP, Business/Economics Universities, Ministry of Economic Development and Technology, Industry Training Organizations.

8. Creation of an International Expansion Fund

Polish cybersecurity firms have high export potential but lack the tools to effectively enter foreign markets. It is recommended to create a dedicated international expansion fund for cybersecurity companies to support participation in trade fairs, local market research, product certification, and the establishment of foreign branches.
Target institutions: Polish Investment and Trade Agency, Ministry of Foreign Affairs, Ministry of Economic Development and Technology, PARP.

9. Development of Innovation-Friendly Public Procurement Mechanisms

The public and defense sectors can act as innovation catalysts, provided that mechanisms are introduced to favor domestic technologies. Recommendations include launching regulatory sandboxes, pre-commercial procurement schemes, and proof-of-concept contracts for SMEs. It is recommended to refrain from mandating references to foreign rankings (e.g., Gartner's "Magic Quadrant"), especially when they do not directly reflect the actual needs of a given procurement. Instead, the use of neutral, open technical and functional criteria is advised, along with a preference for solutions based on local technologies.
Target institutions: Public Procurement Office, Ministry of Digital Affairs, Ministry of Economic Development and Technology, Ministry of National Defence.

10. Harmonizing Interpretation and Supporting EU Legislation Implementation

New legislation such as NIS2, DORA, and CRA are viewed as opportunities but also as a regulatory burden. It is recommended to establish a central information portal with practical guidelines, regularly updated legal interpretations, document templates, and a directory of advisors and auditors.
Target institutions: Ministry of Digital Affairs, Data Protection Authority (UODO), Office of Competition and Consumer Protection (UOKiK), Industry Associations and Chambers of Commerce.

11. Strengthening Industry Organizations and Thematic Consortia

The Polish sector is fragmented and poorly coordinated. It is recommended to support the creation of thematic consortia (e.g. Cybersecurity, Cloud, IoT, AI) to jointly conduct research, export, and advocacy projects. Industry organizations should receive resources to develop their analytical and lobbying capacities. It is also recommended to provide support for the implementation of products into the national cybersecurity system and institutions responsible for State security.
Target institutions: Industry organizations, Ministry of Economic Development and Technology, Ministry of Digital Affairs, PARP.

12. Establishing Cybersecurity Testing Environments (Cyber Sandboxes)

There is a need for controlled environments where companies can simulate threats, test new products, and conduct audits. It is recommended to create regional testing centers accessible to companies, universities, and the military.
Target institutions: Ministry of Digital Affairs, NASK, technical universities, Ministry of National Defence, PARP

13. Building a Joint International Promotion System

A unified brand promoting Polish cybersecurity technologies (e.g. "Polish CyberTech") should be created. This includes a national pavilion at international fairs, a catalog of companies, export promotion, and legal/PR support for entering foreign markets.
Target institutions: Ministry of Digital Affairs, NASK, Technical Universities, PARP.

14. Tax Incentives for Industry and Private Investors

To stimulate investment in the cybersecurity sector, it is recommended to introduce tax incentives for VC/PE funds investing in this domain. Additional preferences could be offered to business angels and public-private co-investment mechanisms.
Target institutions: Ministry of Finance, Ministry of Economic Development and Technology, Polish Investment and Trade Agency.

15. Market Education and Cybersecurity Awareness Promotion

Many recipients still perceive cybersecurity as a non-essential cost. A national awareness campaign is needed, targeting SMEs, municipalities, and public administration, to illustrate the risks, incident costs, and benefits of cybersecurity investment. It should also include PR initiatives showcasing sector success stories, leaders, and innovations.
Target institutions: NASK, Ministry of Digital Affairs, PARP, Industry Organizations, Media / PR Agencies.

16. Strengthening Cooperation with European Structures

Cooperation with European coordinating bodies, such as the European Cybersecurity Competence Centre (ECCC), should be strengthened by improving communication, ensuring the presence of representatives of funding institutions at industry events, and increasing efforts to promote projects co-financed with EU funds. Effective promotion of project results and their broad visibility on the European market can significantly enhance their impact and support the scaling of innovative solutions developed by Polish SMEs.

Target institutions: Ministry of Digital Affairs, National Centre for Research and Development (NCBR), Polish Agency for Enterprise Development (PARP), Polish representatives on the ECCC Governing Board, Ministry of Funds and Regional Policy.

Chapter 1

Overview of the Polish cybersecurity industry

1.1. Mapping the Cybersecurity Sector

The cybersecurity sector in Poland is developing dynamically, driven by a growing number of threats, new legal regulations, and increasing demand for specialized digital protection services. In this context, small and medium-sized enterprises (SMEs) operating in the cybersecurity sector play a key role in delivering innovative solutions. However, they face numerous challenges related to business growth and scaling.

The aim of this study is to identify the key needs of SMEs in the cybersecurity sector and analyze the barriers hindering their growth and competitiveness in the market. The study is based on an analysis of available industry reports, statistical data, and expert publications, allowing for an assessment of the current state of the sector.

Cybersecurity is defined at the national level in the 2018 Act on the National Cybersecurity System as the resilience of information systems to actions that compromise the confidentiality, integrity, availability, and authenticity of the data processed or of services related to such data provided by these systems[1].

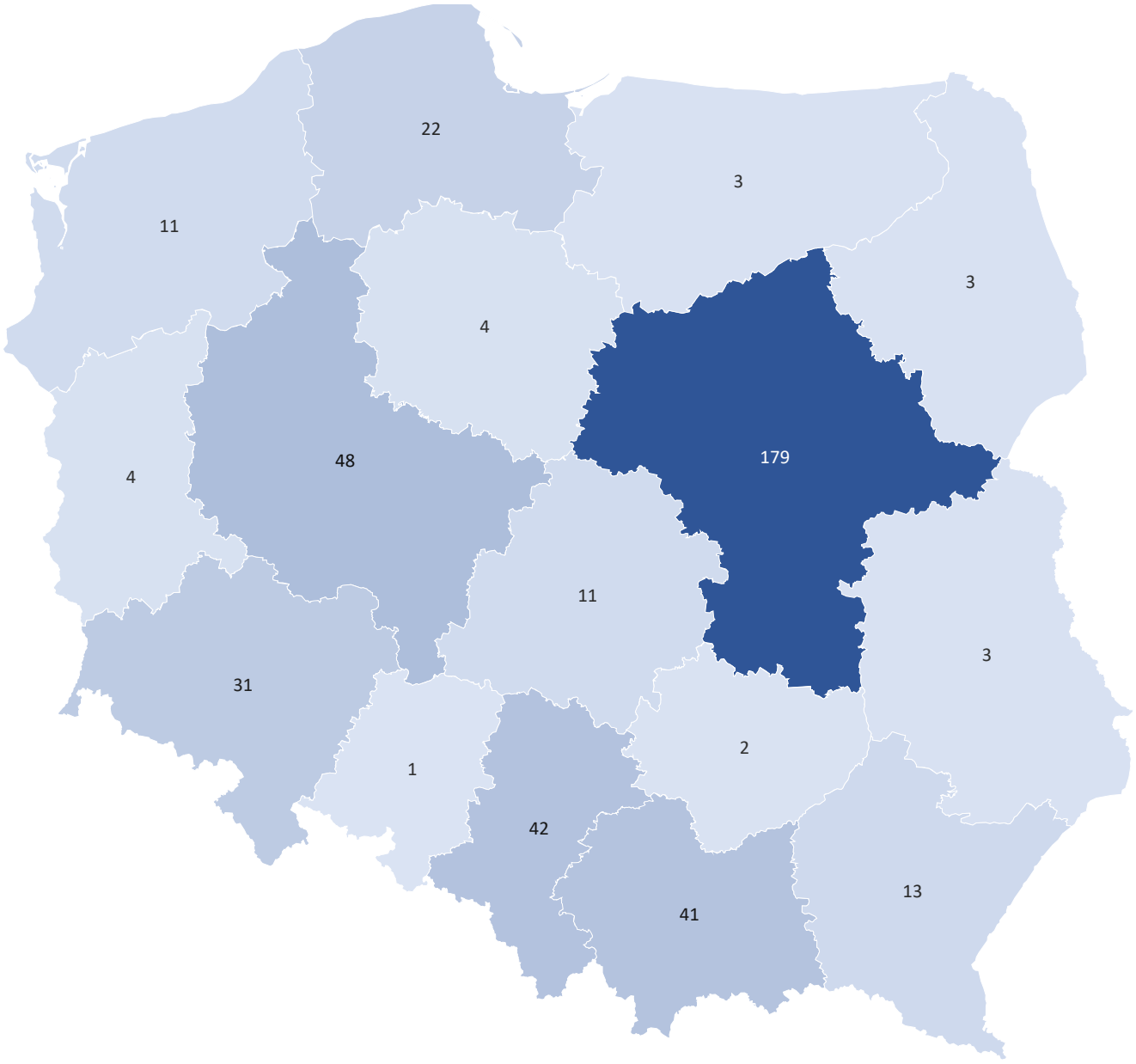
Therefore, a company operating in the cybersecurity sector can be understood as one that delivers products, services, or processes that protect the confidentiality, integrity, availability, and authenticity of data within an organization, or the systems in which such data - including personal and sensitive data - are processed. However, it should be noted that many companies operating more broadly in the field of information technology (IT) offer cybersecurity products or services, but these are not their core business areas. Additionally, there are many companies on the market engaged in reselling cybersecurity products (mostly from foreign vendors), which highlights the fragmented and complex nature of the Polish cybersecurity market and the difficulty of analyzing it uniformly.

According to estimates by The Insights Partners, the global cybersecurity market was valued at approximately USD 203 billion in 2022[2]. These estimates are consistent with data from Statista, which places the market's value at USD 200 billion[3]. Importantly, depending on the source, the projected global compound annual growth rate (CAGR) of this market ranges from 7.5% to even 15%, which could raise its value to USD 660 billion by 2030.[4].

The value of the Polish cybersecurity market in 2025 is estimated at USD 1 billion (approximately PLN 3 billion), representing about 0.5% of the global cybersecurity market. If we include cloud computing, data center services, backup, hosting, and other areas such as physical security, emergency power supply, and forensic IT, the total scale of the Polish market could reach PLN 12 billion[5]. Between 2021 and 2024, the Polish cybersecurity market experienced consistent double-digit growth (11%, 20%, 15%, and 10%, respectively), confirming rising demand for cybersecurity solutions in the country. For the period from 2025 to 2030, the projected CAGR is approximately 6%, which would raise the market's value to PLN 4 billion over five years[6]. These statistics clearly show that the Polish cybersecurity market is expected to grow more slowly compared to the global average.

[1] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Dz.U. 2018, poz. 1560.
[2] Artykuł "Cybersecurity Market Growth to Hit 15.9% CAGR Globally by 2030 – Exclusive Report by The Insight Partners." GlobeNewswire, 8 Nov. 2023. [Access: 17.04.2025]
[3] Cybersecurity – Worldwide. Statista Market Forecast. [Access: 17.04.2025]
[4] Artykuł "Cybersecurity Market Growth to Hit 15.9% CAGR Globally by 2030 – Exclusive Report by The Insight Partners." GlobeNewswire, 8 Nov. 2023. [Access: 17.04.2025]
[5] Artykuł w portalu branżowym "Ekosystem rozwiązań cyberbezpieczeństwa w Polsce wart jest 12 mld zł." ITwiz, 2024. [Access: 17.04.2025]
[6] Artykuł w portalu branżowym "Poland Cybersecurity Market Size & Share Analysis – Growth Trends & Forecasts (2025–2030)." Mordor Intelligence. [Access: 17.04.2025]

Map 1. Geographic Distribution of Cybersecurity Companies



Source: Based on data analyses by IBC Advisory S.A.

The highest number of cybersecurity companies in Poland operate in the **Mazowieckie Voivodeship**, making it the national leader in terms of the number of enterprises active in this sector. Other regions show significantly lower figures: 48 companies are registered in **Wielkopolskie**, 42 in **Śląskie**, 41 in **Małopolskie**, and 31 in **Dolnośląskie**.

Across Poland, the **largest group** of cybersecurity sector entities are **service providers**, with 199 enterprises. They are followed by **system integrators** (129), **vendors** (67), **distributors** (13), and finally, **value added distributors (VADs)** - 10 enterprises. This structure reflects a dominant business model in Poland that emphasizes service delivery and technology integration, with relatively few entities engaged in product manufacturing or distribution.

The most common activity among cybersecurity companies in Poland is **incident monitoring and response** - reported by 209 enterprises. Other major areas include **compliance and security management** (195), **network security** (172), **endpoint protection** (162), **identity and access management** (116), and **security awareness training** (101). Less frequently reported areas include **penetration testing, red teaming, and audits** (107), **vulnerability management** (71), and **cloud security** (51). The rarest specializations are **industrial/OT security** (45 enterprises) and **operation of Security Operation Centers (SOCs)** - 44 enterprises.

It is important to note that a single company may provide services in more than one area - this classification does not imply exclusive categorization. Companies often operate across multiple segments of the market.

In total, **117 enterprises specialize in just one type of service**, while the remaining companies operate in two or more areas. Most commonly, companies offer: **two types** of services - 102 enterprises, **three** - 59 enterprises, **four** – 45 enterprises, **five** - 44 enterprises. Notably, **three companies** were identified as offering **eleven different types of services**, demonstrating a presence of highly diversified market players.

As part of the study, the business profiles of cybersecurity companies were mapped by voivodeship. The analysis revealed **clear regional differences**, both in terms of the number of companies and the types of services offered. The regions requiring special attention due to their concentration of entities are **Mazowieckie, Wielkopolskie, Dolnośląskie, Śląskie,** and **Małopolskie**.

Mazowieckie Voivodeship

Mazowieckie clearly dominates at the national level, with 179 cybersecurity companies. Virtually all business models are represented: service providers, vendors, system integrators, as well as distributors and VADs. Service providers are the largest group, indicating high demand for consulting, implementation, and cybersecurity outsourcing in the region. The presence of vendors and integrators also reflects the development of proprietary solutions and comprehensive technical support. The significant number of companies and their diverse profiles indicate a mature market, especially in Warsaw and its surroundings, which also host the largest cluster of public institutions, data centers, and regulated entities.

Wielkopolskie Voivodeship

Wielkopolskie ranks third in terms of company count (48), with service delivery also being the dominant model. Integrators and vendors are present, though in smaller numbers. Companies in this region most often specialize in penetration testing, incident management, and threat response. The area is growing dynamically, though in a more specialized manner than Mazowieckie - focusing on specific service segments.

Dolnośląskie Voivodeship

Despite having only 31 companies, Dolnośląskie is marked by a high degree of diversity. In addition to 21 service providers, there are 6 vendors, 2 integrators, and 2 distributors. Compared to other regions, Dolnośląskie stands out with a relatively high share of companies offering proprietary solutions or acting as technology intermediaries. This may result from the local concentration of technology and academic centers, especially in Wrocław.

Śląskie Voivodeship

Śląskie, home to 42 cybersecurity companies, is one of the key regional hubs in the sector. A noteworthy aspect is the high number of integrators (18 companies), which suggests strong demand for complex implementations and security system integration, especially among large industrial and manufacturing organizations. The region also includes 16 service providers and 7 vendors, pointing to a robust local technical and human resource base. The sector profile in Śląskie suggests a focus on practical solutions supporting infrastructure and OT security, in line with the region's industrial character.

Małopolskie Voivodeship

Małopolskie, with 41 companies, shows a profile similar to that of Wielkopolskie. The region is dominated by service providers offering a broad range of consulting, audit, and technical services. A few vendors and integrators are also active. The presence of a well-developed education and technology ecosystem in Kraków fosters the growth of local expertise and the emergence of firms providing innovative and specialized services.

1.2. Sector Ecosystem Analysis

To fully understand the dynamics of the market as well as the needs and challenges of Polish SMEs in the cybersecurity sector, it is essential to consider them within the broader ecosystem. Below is a basic analysis highlighting the key institutions and organizations operating in Poland that are most influential in shaping the cybersecurity landscape. These include, among others, the **Ministry of Digital Affairs**, the **Ministry of Economic Development and Technology**, the **National Centre for Research and Development (NCBR)**, **NASK - National Research Institute**, **Institute of Communications - National Research Institute (Iŧ-PIB)**, and the **Institute of Artificial Intelligence and Cybersecurity – Łukasiewicz – AI**.

The **Ministry of Digital Affairs (MC)** has a direct impact on SMEs in the cybersecurity sector primarily through the development of legal frameworks that impose specific obligations on covered entities. This should be viewed both as an opportunity and a challenge for SMEs: regulations can significantly stimulate demand for cybersecurity solutions, yet excessive or unclear regulations may create organizational confusion and raise the cost of implementation for end clients[7]. Additionally, the Ministry develops, updates, and implements the **Polish National Cybersecurity Strategy**. A key initiative for SMEs is the **"Cyber Poland" (PW Cyber) programme**, which serves as a platform for public-private integration, enhancing both visibility and credibility on the market. Moreover, the Ministry's educational and promotional activities increase general awareness of cybersecurity across the economy, contributing to rising demand for SME services. Its international cooperation also opens up opportunities for Polish firms to harmonize with global standards and expand abroad[8]. A key role is also played by **NCC-PL** (National Coordination Centre for Cybersecurity), which actively supports Polish businesses in the European market and serves as the national contact point for activities of the **European Cybersecurity Competence Centre (ECCC)**.

The Ministry of Economic Development and Technology (MRiT), as the main institution responsible for shaping the country's economic and innovation policies, is another crucial part of the cybersecurity ecosystem - particularly in terms of financial and programme support for SMEs seeking to invest in cybersecurity or develop their own products and services in this area. This includes grant programmes, tax incentives, and improved access to capital.
Furthermore, the Ministry shapes trade and investment policies, works to increase the competitiveness of the Polish economy on the international stage, and engages in dialogue with businesses and social partners[9].
Two key agencies operate under the Ministry: the **Polish Agency for Enterprise Development (PARP)**, and the **Polish Investment and Trade Agency (PAIH)**. Both institutions offer dedicated support programmes to help SMEs grow and expand.

The **National Centre for Research and Development (NCBR)** is an executive agency of the Ministry of Science and Higher Education and plays a central role in funding and supporting scientific research and development in Poland. NCBR actively funds projects across various fields, identifying strategic development directions and investing in innovative solutions. For SMEs conducting R&D in cybersecurity, NCBR is a vital source of funding that enables the development of new products and services, enhances competencies, and strengthens market position. The agency also helps SMEs establish partnerships with research institutions[10].

The Scientific and Academic Computer Network – National Research Institute (NASK-PIB) operates under the supervision of the Ministry of Digital Affairs. As a state research institute, NASK-PIB undertakes tasks at the intersection of science, technology, and public administration, supporting the state in areas such as monitoring threats in cyberspace, raising digital awareness, protecting children online, and implementing innovative solutions in the field of ICT security. In accordance with its statute, NASK-PIB conducts scientific research and development work within a defined scope, adapts their outcomes to practical needs, and implements them in services provided, among others, to national security and public order institutions. Additionally, the Institute conducts conformity assessments, carries out certification processes, and engages in standardization activities.

[7] Raport "Polski rynek cyberbezpieczeństwa 2023–2028". Polski Klaster Cyberbezpieczeństwa #CyberMadeInPoland, Październik. 2023, s. 128.
[8] Strona internetowa Ministerstwa Cyfryzacji - Działania, Gov.pl. [Access: 26.06.2025]
[9] Strona internetowa Ministerstwa Rozwoju i Technologii - działania ministerstwa, Gov.pl. [Access: 26.06.2025]
[10] Strona internetowa Narodowego Centrum Badań i Rozwoju, Gov.pl. [Access: 26.06.2025]

NASK-PIB plays a key role in the area of security certification, holding competences in Common Criteria (CC) – the international standard for evaluating the security of IT products and systems. The NASK Certification Body is the only institution in Poland authorized to issue international Common Criteria certificates, which assess the security of IT products and systems. The CC standard is used by governments and companies worldwide to evaluate the safety of technologies. As part of its support for SMEs, the institute also runs the "Digitally Secure Company" program, aimed at improving cybersecurity in small and medium-sized enterprises through audits, training, and best practices. Upon completion of the improvement activities, a company can apply to the NASK Certification Body to begin the certification process under this program.

Within the structure of the national cybersecurity system, NASK operates CSIRT NASK – one of three national-level computer security incident response teams, alongside CSIRT GOV (operated by the Internal Security Agency) and CSIRT MON (operated by the Ministry of National Defence).

According to **Article 26 of the Act**, CSIRT-NASK is responsible for, among other:

- Coordinating the handling of incidents reported by designated entities,
- Creating and providing tools for voluntary cooperation and information exchange on cybersecurity threats and incidents,
- Operating a telephone hotline or web service for reporting and analyzing cases of the distribution or transmission of child sexual abuse material through ICT technologies[11],

as well as:

- Monitoring cybersecurity threats related to ICT networks and systems,
- Receiving incident reports and supporting entities in incident response,
- Analyzing incidents, threats, and their consequences,
- Exchanging threat intelligence with other entities in the national cybersecurity system, including CSIRT GOV and CSIRT MON,

Additionally, NASK-PIB may engage in training, exercises, educational campaigns, and preventive activities aimed at raising cybersecurity awareness.

NASK-PIB serves as a bridge between academia, technology, and public administration, supporting the state's efforts in areas such as cybersecurity, digital education, child online protection, cyber threat monitoring, and coordination of incident response in public administration networks and among key and important service providers.

The **Institute of Communications - National Research Institute (IŁ-PIB)** is an independent national R&D unit specializing in telecommunications and information technologies. The Institute cooperates actively with national and international research centers, supporting scientific collaboration and contributing to the development of the **European Research Area (ERA)**. Its activities supporting the private sector mainly include certification processes, compliance testing, technical documentation support, and preparation of declarations of conformity. Its research has both developmental and applied dimensions[12].

The **Łukasiewicz Research Network - Institute of Artificial Intelligence and Cybersecurity – Łukasiewicz – AI** is one of Poland's leading research institutes and part of the **Łukasiewicz Research Network**. The institute conducts scientific and development work to create solutions for industry, public administration, and the defense sector. The institute is a potential R&D partner for SMEs, offering access to specialized knowledge and research infrastructure. The AI Institute also offers services to support the Common Criteria certification process and, together with the Institute of Communications, acts as a conformity assessment body under this scheme. SMEs can collaborate with the institute to develop innovative cybersecurity products and services, particularly in the context of industrial systems (OT/ICS). The institute may also provide training and consulting, supporting SMEs in improving both their technological capabilities and business competencies[13].

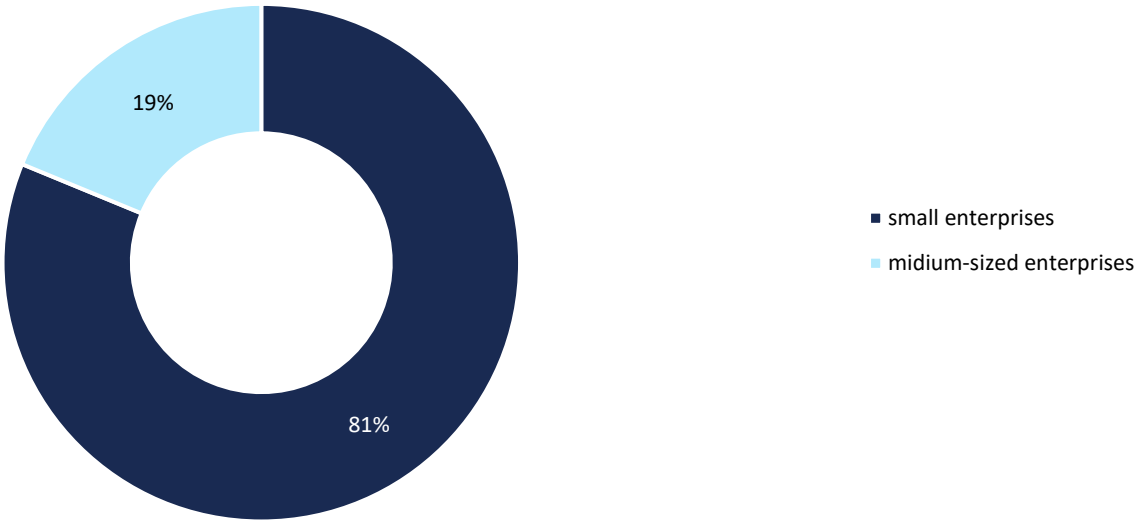
[11] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Dz.U. 2018, poz. 1560. s.26-28.
[12] Strona internetowa Instytutu Łączności – Państwowego Instytutu Badawczego, Gov.pl. [Access: 18.04.2025]
[13] Strona internetowa Łukasiewicz – AI, Gov.pl. [Access: 04.07.2025]

1.3. Overview of Small and Medium Enterprises in Poland's Cybersecurity Sector

A total of 201 enterprises participated in the quantitative study, classified by company size. The survey was completed by 197 firms, while 20 company representatives took part in in-depth interviews – including four entities that did not participate in the quantitative survey. Respondents were divided into two categories: small and medium-sized enterprises. The distribution of companies in the sample is as follows:

- Small enterprises - 160 companies - defined as entities employing fewer than 50 people on average annually and whose annual net turnover from the sale of goods, products, services, and financial operations does not exceed the PLN equivalent of EUR 10 million, or whose total annual balance sheet does not exceed the equivalent of EUR 10 million.
- Medium-sized enterprises - 37 companies - defined as entities employing fewer than 250 people on average annually and whose annual net turnover from the sale of goods, products, services, and financial operations does not exceed the PLN equivalent of EUR 50 million, or whose total annual balance sheet does not exceed the equivalent of EUR 43 million, and which are not small enterprises.

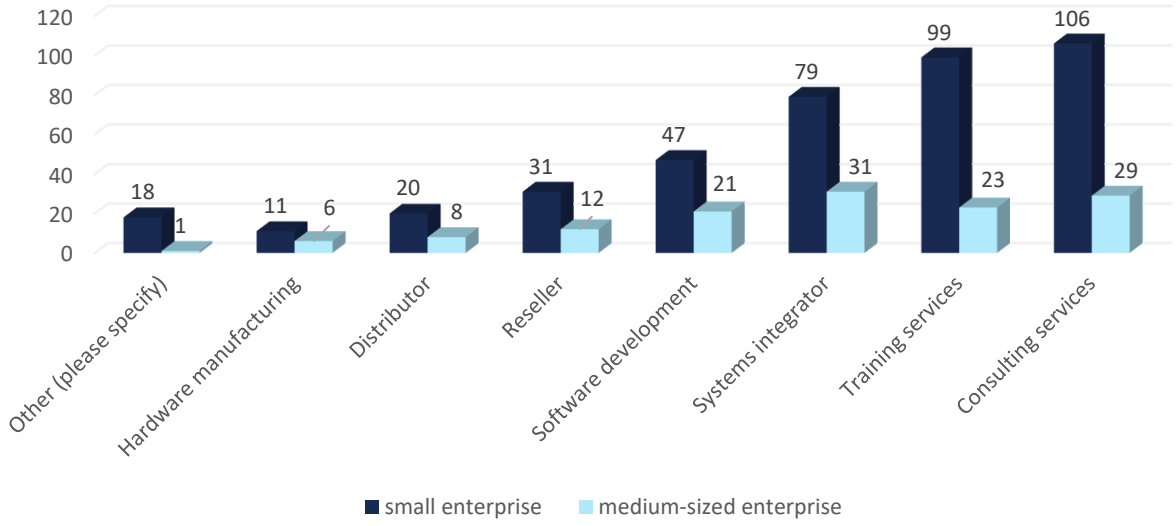
Chart 1. What is the size category of the enterprise? (N=197)



Source: IBC Advisory S.A. analyses based on CAWI survey.

Next, respondents in the CAWI survey were asked about the type of business activity they conduct within the cybersecurity sector. The question allowed multiple selections, enabling companies to indicate all areas in which they are active.

Chart 2. Types of Business Activity in the Cybersecurity Sector (N=197)



Source: IBC Advisory S.A. analyses based on CAWI survey.

The responses indicate a high degree of diversity in the services provided and products offered by the surveyed companies. The most frequently indicated activities among small and medium-sized enterprises were:

- Consulting services (106 from small and from 29 medium-sized enterprises),
- Training services (99 from small and from 23 medium-sized enterprises),
- Security solution integration (79 from small and from 31 medium-sized enterprises),
- Software development (47 indications from small enterprises and 21 from medium-sized enterprises),
- Reselling and distribution (51 from small and from 20 medium-sized enterprises),
- Hardware manufacturing (11 from small and 6 from medium-sized enterprises).

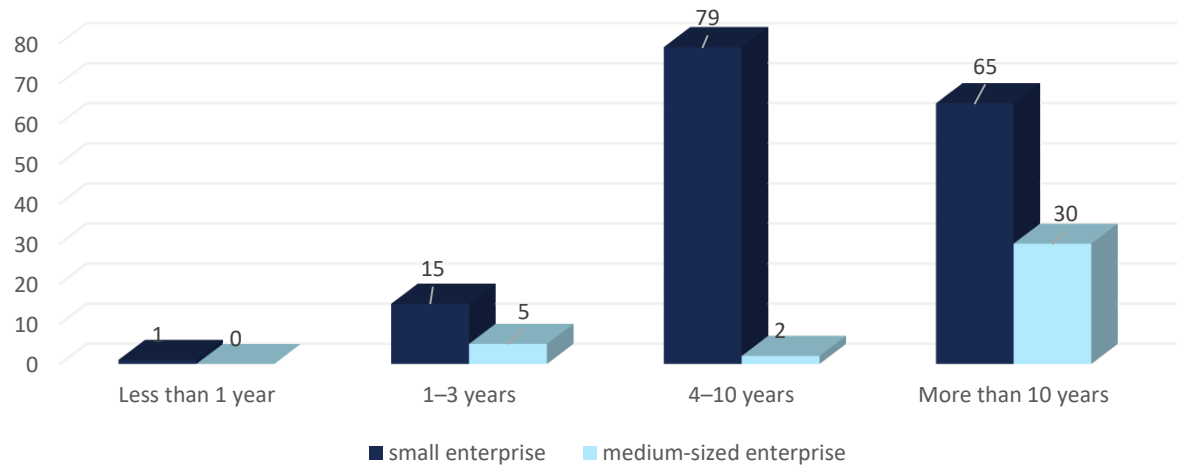
In open-ended responses:

- Managed security services (MSSP, SOC, MDR),
- Security and penetration testing,
- IT service outsourcing,
- Specialized services related to critical infrastructure (NIS2),
- Telecommunication activities and software testing.

These results show that many companies operate across multiple market segments, offering both services and products, which confirms the complex structure of the Polish cybersecurity market.

The chart below presents the market tenure of the surveyed companies, i.e. how long the enterprises have been operating in the market.

Chart 3. How many years has the company been operating in the market? (N=197)



Source: IBC Advisory S.A. analyses based on CAWI survey.

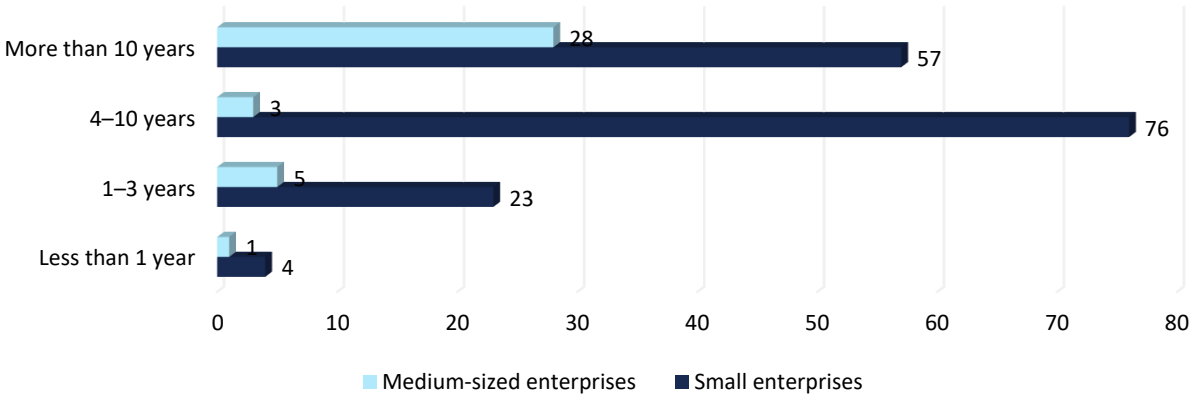
The vast majority of companies active in the cybersecurity market are long-established entities. Among small enterprises, the largest group consists of firms that have been operating for 4 to 10 years - 79 companies. Another 65 small businesses have been active for over 10 years. Younger companies are less common: 15 have operated for 1 to 3 years, and only 1 company for less than a year.

For medium-sized enterprises, the dominant group includes those with the longest market tenure - 30 companies have been in operation for over 10 years. Significantly fewer medium-sized companies have shorter experience: 5 have operated for 1 to 3 years, and only 2 for 4 to 10 years. No medium-sized companies in the sample have been active for less than a year.

These figures indicate that the majority of SMEs in the cybersecurity sector have several years or even over a decade of experience, while the share of newly established companies is relatively small. This may suggest that cybersecurity operations are most commonly developed by well-established and experienced firms.

The chart below shows how long the surveyed companies have been active specifically in the field of cybersecurity. These data illustrate the level of experience in this particular domain, which may affect a company's competencies, service offerings, and market position.

Chart 4. How many years has the company been active in the field of cybersecurity? (N=197)



Source: IBC Advisory S.A. analyses based on CAWI survey.

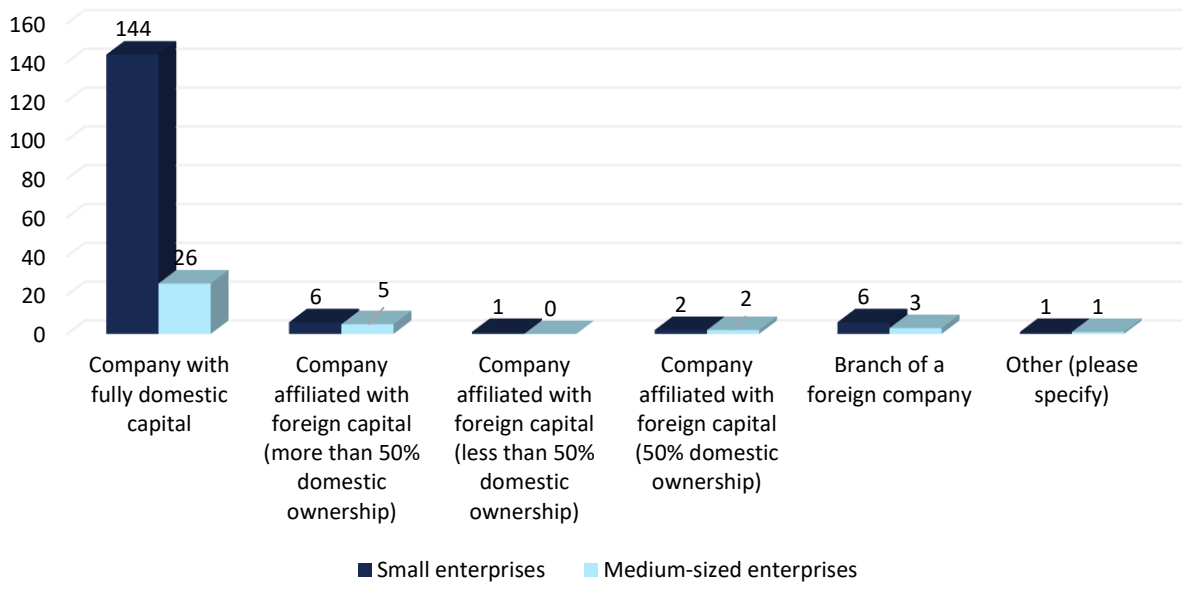
Among small enterprises, the largest group consists of companies that have been active in the cybersecurity sector for 4 to 10 years - 76 firms. Another significant category includes companies that have operated in this field for over 10 years (57 firms). A total of 23 small companies entered the cybersecurity field within the last 1-3 years, and 4 firms have been active for less than a year. This suggests that while some companies may have existed earlier, their cybersecurity-related operations began at a later stage in their development.

In the case of medium-sized enterprises, the majority (28 companies) have been active in cybersecurity for over 10 years. Fewer companies started their cybersecurity operations 1-3 years ago (5 firms) or 4-10 years ago (3 firms), while only 1 company has been active in this area for less than a year.

These findings indicate that both small and medium-sized enterprises typically have long-standing experience in the cybersecurity field - although not necessarily from the moment the company was founded. Most companies began operating in the sector at least four years ago, which may reflect market stabilization and a growing specialization in response to increasing demand for digital security services.

The chart below illustrates the ownership structure of the surveyed companies. The vast majority of respondents were companies with entirely domestic capital. The share of enterprises with any form of foreign capital participation was relatively low.

Chart 5. Type of company ownership: (N=197)



Source: IBC Advisory S.A. analyses based on CAWI survey.

The vast majority of companies surveyed were entities with entirely domestic capital. This ownership structure was declared by 144 small and 26 medium-sized enterprises, indicating that the Polish SME cybersecurity sector is primarily built on domestic firms.

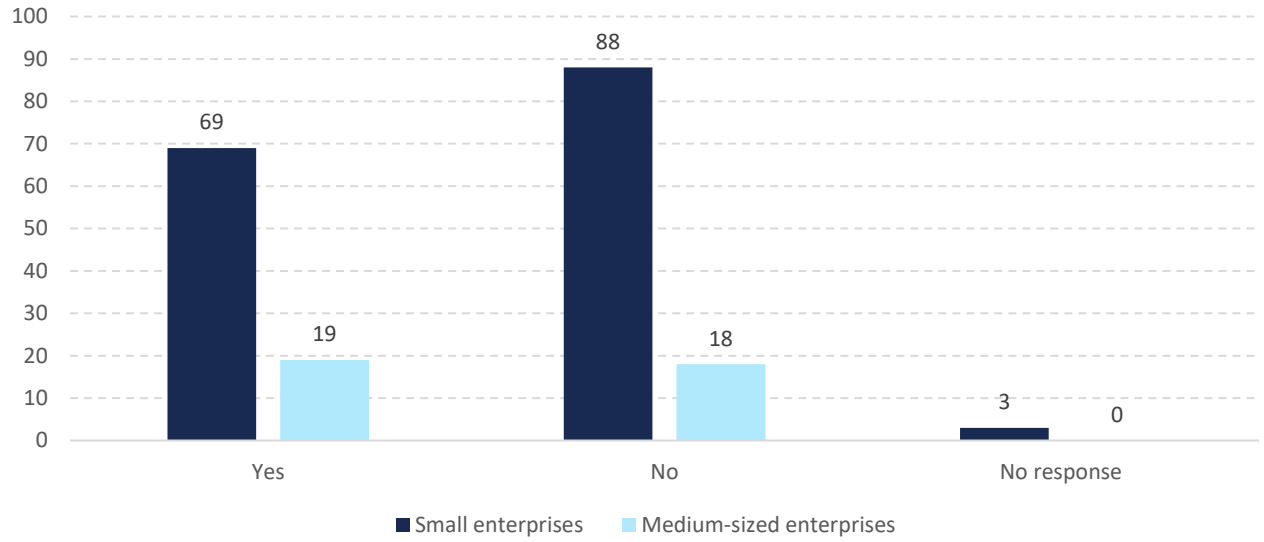
Other forms of capital ownership were far less common. Companies with foreign capital involvement, in which more than 50% of shares remain in domestic hands, were reported by 6 small and 5 medium-sized firms. Only one small company reported that less than 50% of its capital was of domestic origin, and no such cases were recorded among medium-sized enterprises. Two small and two medium-sized companies declared an even (50/50) split between domestic and foreign capital.

The sample also included 6 small and 3 medium-sized enterprises that are branches of foreign companies. Non-standard ownership forms, marked as “Other”, were selected by one respondent from each group.

These findings clearly indicate that domestic ownership prevails among SMEs operating in the cybersecurity sector in Poland, while foreign capital involvement is relatively rare.

Another surveyed aspect was company membership in industry organizations, such as clusters or chambers of commerce. Affiliation with such structures may facilitate knowledge exchange, collaboration, and joint cybersecurity initiatives. The survey asked respondents whether their company is a member of such an organization.

Chart 6. Is your company a member of any industry organization (e.g. cluster, chamber of commerce)? (N=197)



Source: IBC Advisory S.A. analyses based on CAWI survey.

The majority of companies participating in the survey are not members of any industry organizations, such as clusters or chambers of commerce. A total of 88 small and 18 medium-sized enterprises declared no affiliation. In contrast, 69 small and 19 medium-sized companies confirmed membership in such organizations. This indicates that while a portion of enterprises recognizes the value of participating in industry structures, a stance of organizational independence still prevails.

These results suggest that despite the existence of structures supporting cooperation and sectoral representation, a significant number of cybersecurity SMEs in Poland operate outside of such frameworks.

Among companies where cybersecurity is the core activity, a wide range of solutions can be identified. Given the fragmentation of the Polish cybersecurity market, for the purposes of this analysis, small and medium-sized enterprises were grouped into 12 of the most common solution categories.

1. **Endpoint Security** - This category includes solutions focused on securing user-end devices such as desktops, laptops, tablets, and smartphones - tools that are among the most common attack vectors. As such, endpoint protection is a critical component of IT security strategies. These solutions aim to detect and block malware, prevent unauthorized access, and monitor for anomalous user behavior.
   Endpoint security tools address vulnerabilities related to ransomware, phishing, malware, and unintentional data leaks caused by users. Modern solutions go beyond traditional antivirus software and increasingly rely on behavioral analytics, artificial intelligence, and automated incident response[14].
2. **Network Security** - Network security encompasses a set of technologies, policies, and practices designed to protect the confidentiality, integrity, and availability of network infrastructure and the data it carries. As organizations of all sizes depend on network systems to deliver services and manage data, securing this infrastructure is essential. Core technologies in this area include: Firewalls - which filter traffic based on predefined rules, IDS/IPS systems -

[14] Artykuł "Threat Landscape for Endpoint Security". ENISA, 2023. [Access: 17.04.2025]

Intrusion Detection/Prevention Systems that detect and block suspicious activity, and Network segmentation tools - which limit the spread of threats. More advanced solutions like NDR (Network Detection and Response) provide real-time analysis and incident response capabilities[15].

3. **Identity and Access Management (IAM)** - IAM refers to the policies, processes, and technologies that allow organizations to control who has access to what digital resources, under what conditions, and with what permissions. These systems are essential for preventing unauthorized access, reducing the risk of data breaches, and ensuring regulatory compliance. IAM solutions support the full identity lifecycle - from account creation and role assignment to deactivation - enabling organizations to manage user access securely and efficiently[16].
4. **Cloud Security** - Cloud security encompasses a set of tools, technologies, and practices that protect data, applications, and services stored in the cloud from threats such as data loss, unauthorized access, or DDoS attacks. With the growing popularity of cloud-based solutions, ensuring a high level of security has become critical - particularly when handling sensitive information. Key mechanisms used in cloud security include: Data encryption, Access control, Identity and Access Management (IAM), and User activity monitoring and auditing[17].
5. **Penetration Testing, Red Teaming, and Security Audits** - These are key security assessment techniques that help organizations identify vulnerabilities before they are exploited by malicious actors. Penetration testing involves simulating external attacks to identify weaknesses in applications, networks, and infrastructure. Red Teaming offers a more comprehensive approach by mimicking advanced threat actors, such as organized cybercriminal groups. It tests not only technology but also processes and personnel readiness. Security audits are thorough reviews of an organization's systems and procedures to evaluate compliance with standards, internal policies, and industry best practices[18].
6. **Vulnerability Management** - Vulnerability management is the process of identifying, assessing, classifying, and eliminating weaknesses in IT systems to reduce the risk of exploitation by cybercriminals. Key components of this process include asset inventory, regular vulnerability scanning, risk analysis, prioritization, and remediation through the application of appropriate patches and updates.
   Vulnerability management tools support automated detection and response, enabling organizations to effectively monitor and secure their IT infrastructure[19].
7. **Incident Monitoring and Response** - This involves the continuous monitoring of IT systems to detect suspicious activities and provide a rapid response to emerging threats. The goal is to quickly identify and neutralize incidents such as hacking attempts, malware infections, or unauthorized access.
   Monitoring tools enable the collection, analysis, and correlation of data from various sources, allowing for faster detection and response. Incident response actions may include isolating affected systems, conducting forensic investigations, and implementing remediation measures[20].
8. **Security Awareness and Training** - Employee education and awareness-building are critical components in protecting organizations against threats stemming from human error. The aim of these initiatives is to educate staff on security best practices, recognize threats such as phishing or social engineering, and respond appropriately to suspicious situations. Training programs may include e-learning modules, workshops, scenario-based tests, and attack simulations. Well-structured and regular training significantly increases organizational awareness and helps reduce the risk of user-targeted cyberattacks[21].
9. **Compliance and Security Management (Consulting)** - This area helps organizations comply with applicable regulations while ensuring robust information security practices. Core activities include the implementation of policies, procedures, and standards related to data protection (e.g., GDPR) and information security management (e.g., ISO/IEC 27001). Companies conduct compliance audits, monitor adherence to regulations, and evaluate

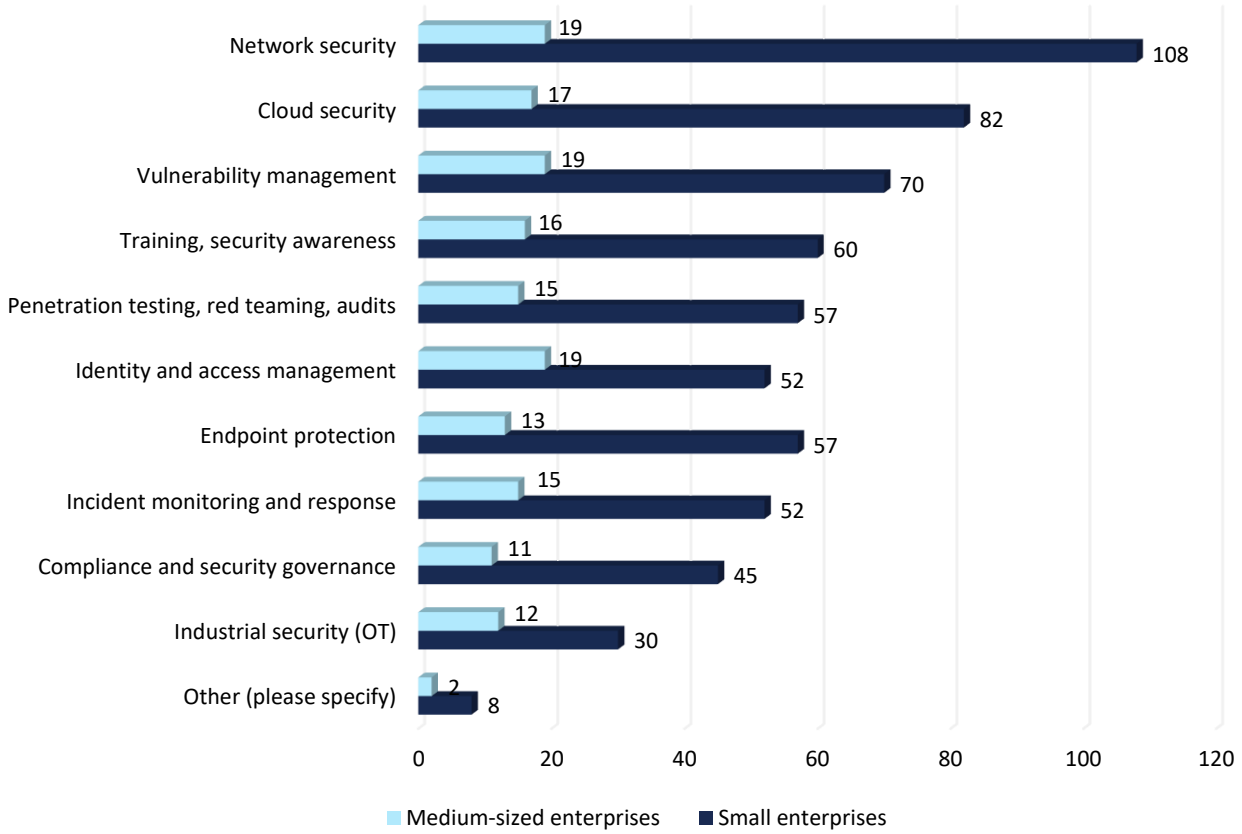
[15] Artykuł "Network and Information Security Threat Landscape". ENISA, 2023. [Access: 17.04.2025]
[16] Artykuł "Co to jest zarządzanie dostępem i tożsamościami?". Microsoft, 2025. [Access: 17.04.2025]
[17] Artykuł "Bezpieczeństwo w chmurze". Microsoft, 2025. [Access: 17.04.2025]
[18] Artykuł "Penetration Testing and Red Teaming". ENISA, 2023. [Access: 17.04.2025]
[19] Publikacja "Vulnerability Management". Qualys, 2023.[Access: 17.04.2025]
[20] Artykuł "Digital Forensics and Incident Response Retainer Services Reviews and Ratings". Gartner, 2025. [Access: 17.04.2025]
[21] Artykuł "Security Awareness Training". SANS Institute, 2025. [Access: 17.04.2025]

information security risks. These efforts minimize the risk of breaches and ensure business continuity. Consulting services in this area support companies in adapting their processes to evolving legal and regulatory requirements[22].

10. **Operational Technology (OT) Security** - OT security focuses on the protection of systems and devices used in industrial infrastructure, such as control units, sensors, and monitoring systems. The goal is to ensure the integrity, availability, and confidentiality of these systems against cyber threats.
    This includes access control, incident monitoring and detection, and regulatory compliance. OT protection is especially critical in sectors such as energy, manufacturing, and transportation, where system failures can have severe consequences[23].
11. **Security Operation Center (SOC)** - A SOC is a dedicated facility responsible for monitoring, analyzing, and responding to cybersecurity incidents within an organization. Staffed by security analysts and engineers, SOC teams typically operate 24/7 to safeguard against cyber threats. Their responsibilities include network and system monitoring, incident analysis, and coordinating response efforts, ensuring the rapid detection and mitigation of potential attacks[24].
12. **Other** - The "Other" category includes services, solutions, and processes that do not fall into any of the categories above. It also covers companies whose offerings are not directly related to cybersecurity, such as providers of ERP or CRM systems, server infrastructure, or hosting services.

Next, respondents were asked about the technologies and services being developed within their companies in the field of cybersecurity. The following data show which areas attract the most attention and investment, as well as what niche solutions are present in the sector.

Chart 7. What technologies/services are being developed by your company? (N=197)



Source: IBC Advisory S.A. analyses based on CAWI survey.

[22] Artykuł "Building Trust for Today and Tomorrow". PwC, 2025. [Access: 17.04.2025]
[23] Artykuł "What Is Operational Technology (OT) Security?". Cisco, 2025. [Access: 17.04.2025]
[24] Artykuł "What Is a Security Operations Center (SOC)?". IBM, 2024. [Access: 17.04.2025]

The survey respondents, representing small and medium-sized enterprises in the cybersecurity sector, most frequently indicated that they develop technologies and services related to network security. This category was selected by 82 small and 19 medium-sized enterprises, making it the most commonly developed area among the surveyed companies.

The next most frequently mentioned areas were:

- Identity and access management (70 small and 17 medium-sized firms),
- Training and security awareness services (60 small and 19 medium-sized firms),
- Penetration testing and security audits (57 small and 16 medium-sized firms),
- Endpoint protection (57 small and 13 medium-sized firms).

A significant number of respondents are also working on:

- Threat monitoring and detection solutions (52 small and 15 medium-sized firms), and
- Security incident management (52 small and 19 medium-sized firms).

Other, less commonly indicated but still relevant areas include:

- Compliance and audit services (45 small and 11 medium-sized firms), and
- General information security solutions (30 small and 12 medium-sized firms).

A smaller number of responses fell under the “Other” category (10 companies), but included interesting examples such as:

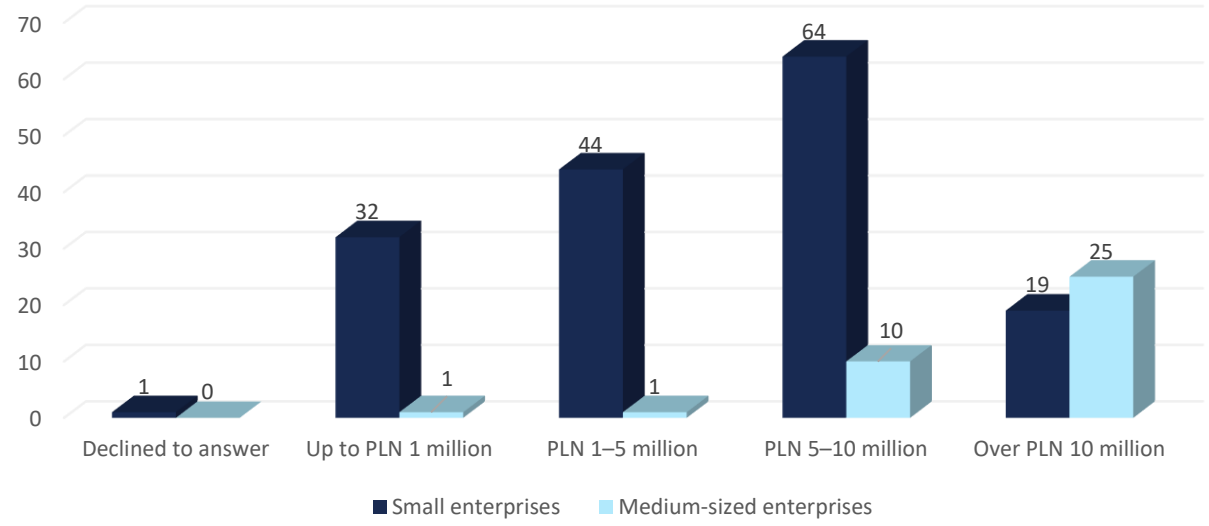
- Data destruction technologies,
- Anti-jamming/spoofing GPS synchronization solutions,
- ISAC and CTI platforms,
- Managed security and 24/7 SOC services,
- End-to-end encryption tools,
- Legal advisory for AI developers,
- And niche software, e.g., for the railway industry.

The findings show that companies place the greatest emphasis on the core pillars of IT security - network protection, cloud security, and vulnerability management. At the same time, educational and preventive measures are gaining increasing importance. The less common but innovative solutions highlight the emergence of specialized and niche technologies within the industry.

It is also worth noting that among medium-sized enterprises, the responses were fairly evenly distributed across different technology categories. While network security, vulnerability management, and identity/access management were the most frequently mentioned (each with 19 responses), other areas such as training, penetration testing, incident management, and threat monitoring were also similarly popular, with only minor differences in response counts. This suggests a broadly diversified activity profile among medium-sized companies in the sample.

Next, respondents were asked to indicate the range of their annual revenues. This information helps to better understand the financial profile of the surveyed entities.

Chart 8. What is the company's annual revenue range? (N=197)



Source: IBC Advisory S.A. analyses based on CAWI survey.

Respondents were asked to indicate their company's annual revenue range. The largest number of companies reported revenues between PLN 5-10 million, with 64 small and 10 medium-sized enterprises falling within this category.

The next most frequently selected category among small firms was PLN 1-5 million (44 responses), followed by revenues up to PLN 1 million (32 responses). In the case of medium-sized enterprises, these ranges were marginal - each selected by only one company.

The highest revenue bracket, above PLN 10 million, was indicated by 19 small and as many as 25 medium-sized enterprises, suggesting that among the surveyed medium-sized firms, those with relatively high revenues dominate.

Only one small company did not provide a response to this question.

These results show that while revenue levels among small enterprises vary significantly, medium-sized firms in the sample are more likely to report annual revenues exceeding PLN 10 million.

The Polish SME cybersecurity sector is highly diverse and fragmented. The market includes companies offering products strictly focused on information security and privacy protection; firms providing services such as auditing and regulatory compliance; as well as those integrating multiple solutions within comprehensive IT systems.

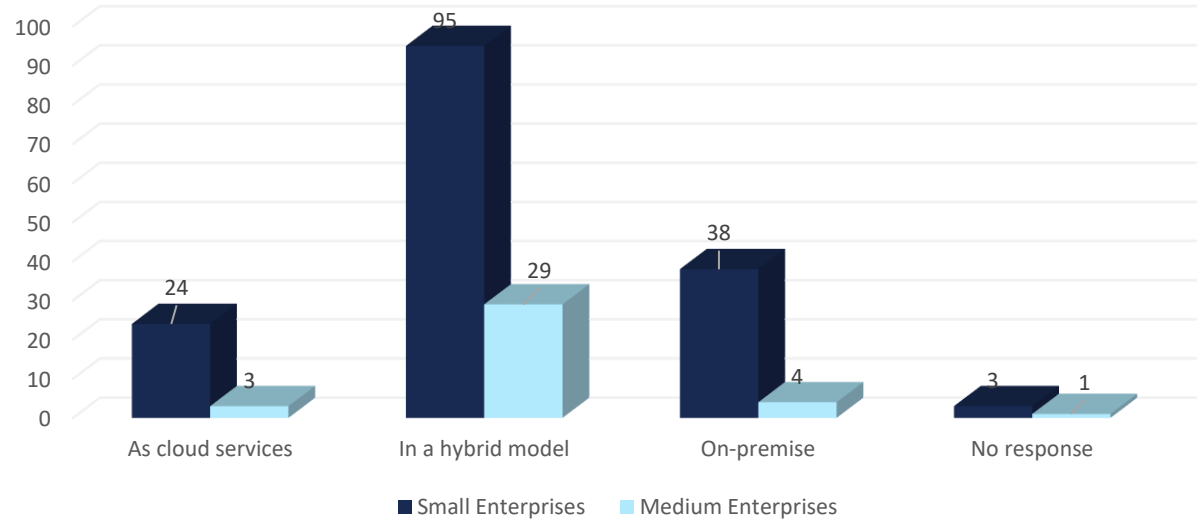
Additionally, cybersecurity products and services are often offered by companies for which cybersecurity is not the primary area of business - but rather an extension of services in software development, cloud infrastructure, or hosting.

1.4. Business models

The methods of delivering products and services, as well as sales and distribution models, play a key role in the development strategies of companies in the cybersecurity sector. With the growing popularity of cloud-based solutions and changes in how customers purchase technology, companies must flexibly adapt their approaches to meet market expectations. At the same time, cooperation with commercial partners and the distribution of solutions developed by other domestic producers can be an important factor in strengthening competitive positioning and supporting the innovation ecosystem. The following charts present the most commonly used models for product delivery, the use of sales intermediaries, and collaboration with other Polish companies in offering technological solutions. These results help identify prevailing market approaches and potential areas for further development.

The chart below presents the preferred product delivery models used by companies in the cybersecurity sector. The most common approach is a **hybrid model**, combining cloud and on-premise solutions, which may indicate a flexible, customer-centered strategy.

Chart 9. Do you offer your products as cloud services, on-premise solutions, or in a hybrid model? (N=197)



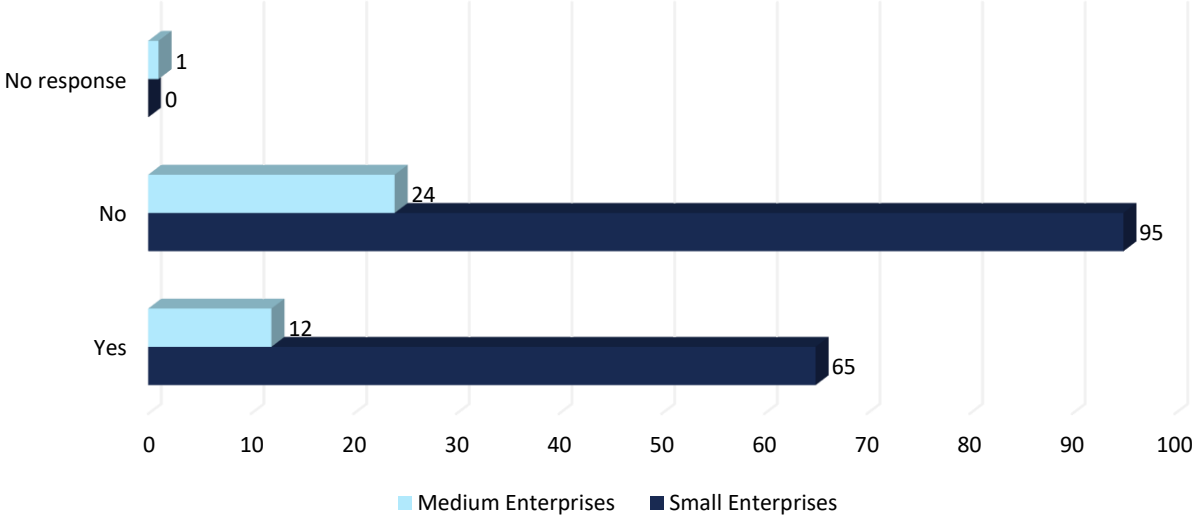
Source: IBC Advisory S.A. analyses based on CAWI survey.

The most frequently indicated model was the hybrid offering, combining on-premise and cloud-based solutions. This response was selected by 95 small and 29 medium-sized enterprises.

On-premise-only solutions are offered by 38 small and 4 medium-sized companies, while cloud-only services are provided by 24 small and 3 medium-sized enterprises.

These results indicate that the cybersecurity market tends to favor a mixed approach, reflecting the diverse needs of clients and a gradual, though not yet complete, adoption of cloud-based services.

Chart 10. Do you use sales intermediaries such as integrators, distributors, or resellers? (N=197)



Source: IBC Advisory S.A. analyses based on CAWI survey.

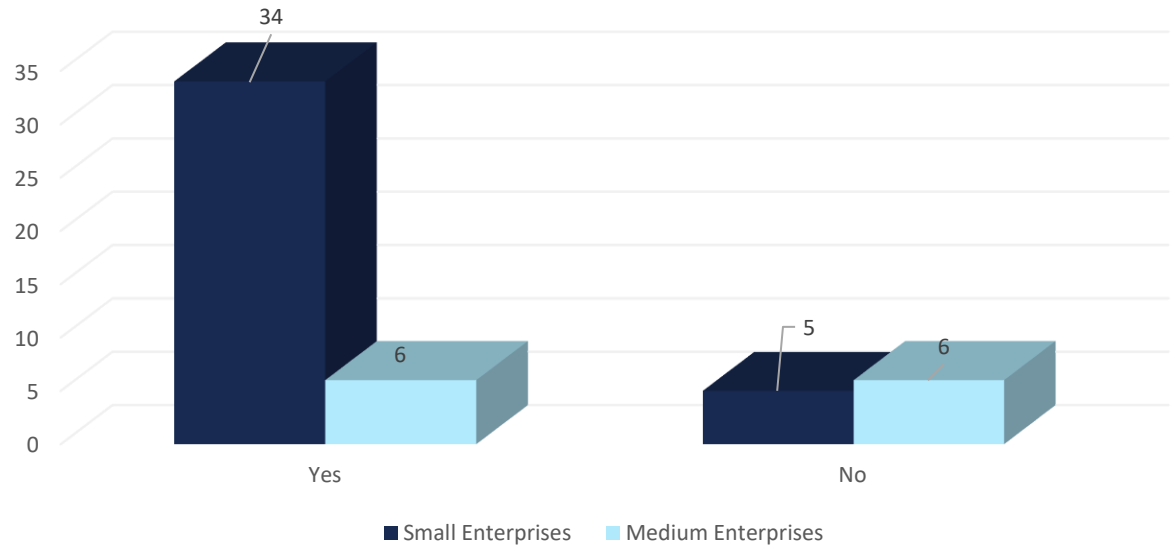
Most companies - both small and medium-sized - declared that they do not use this type of distribution channel. The answer “no” was selected by 95 small and 24 medium-sized enterprises.

Sales intermediaries are used by 65 small and 12 medium-sized companies, which means that although it is a less common form of distribution, it is still employed by a significant portion of the surveyed entities.

These results suggest that while direct sales models dominate, a considerable number of firms use partner networks, which may be linked to efforts to reach broader markets, optimize sales costs, or compensate for limited internal resources. An intermediary model may also indicate more developed distribution structures within the cybersecurity sector.

Respondents were then asked whether they offer products/services/technologies developed by other domestic companies. As shown in the results below, most enterprises do offer such products.

Chart 11. Do you offer products/services/technologies developed by other domestic companies? (N=51)



Source: IBC Advisory S.A. analyses based on CAWI survey.

Out of the 51 companies that responded to this question, the majority declared cooperation in the distribution or integration of solutions developed by other Polish entities. Such products are offered by 34 small and 6 medium-sized enterprises, totaling 40 firms. In contrast, 11 companies (5 small and 6 medium-sized) stated that they do not offer Polish products.

These results may suggest that most companies do not limit themselves to foreign solutions, but actively leverage the achievements of domestic firms, which can support innovation and enhance the competitiveness of the entire sector.

Chapter 2

Strengths and Prospects of Domestic Cybersecurity SMEs

2.1. Human Resources and Competencies (based on ECSF)

The in-depth interviews included both very small companies, employing from a dozen to several dozen people, as well as more technologically advanced enterprises. As one respondent described:

"[...] to this day, the company employs several dozen people. These are usually engineers, technical support, people responsible for new products and solutions [...]" ~ Respondent 3.

Another company, operating on the borderline of the SME category, reported employing close to one hundred people, including collaboration with academic staff:

"Currently, about 80 people are employed in the company's operations. Not all of them are full-time employees; we also work with academics, professors, habilitated doctors [...]" ~ Respondent 15.

Many company representatives noted that the traditional full-time employment model is no longer dominant. Especially in small and medium-sized enterprises, flexible collaboration models are preferred-based on B2B contracts, task-based arrangements, commissioned work, or project-based billing models.

"As for employment, we don't have the classic full-time contracts [...] all the people we work with are trusted and have been with us for a long time [...]" ~ Respondent 7.

Most of the companies participating in the study declared the use of diverse forms of employment and collaboration, reflecting the growing trend toward flexible human resource management. Alongside traditional employment contracts, B2B agreements, civil law contracts, task-based work, and project-based models are becoming increasingly common. This diversity allows organizations to swiftly adjust their staffing to current operational needs and better control personnel costs. Companies can scale their workforce up or down depending on project intensity, without incurring long-term obligations.

In practice, this results in significant differences between the number of full-time employees and the total number of individuals actually involved in project execution and daily operations. According to respondents, the core full-time team in some companies consists of just a dozen people, while during peak project periods, the number of collaborators can double.

"At this moment, we employ around 12 people under regular contracts, and we also have individuals working under B2B arrangements." ~ Respondent 1.

This approach is fully justified given the specific characteristics of the cybersecurity sector, which often involves a high degree of specialization and great variability and unpredictability in client orders-from both private and public sectors. The diversity of project requirements and the fluctuation of their timelines necessitate flexibility and the ability to respond quickly. Therefore, adopting a flexible employment model not only enhances operational efficiency but also reflects organizational maturity-indicating a strategic approach to human capital management in terms of process optimization and maximizing business effectiveness.

Employment scale depends on the company's development phase and business profile

Larger organizations, serving both domestic and international markets, typically have a broader portfolio of projects and services, which translates into a significantly higher number of collaborators-ranging from 60 to even 100 people. It is important to note that this number includes not only full-time employees but also B2B contractors and external experts, including members of the academic community.

"At the moment, the company employs about 80 people. Not all of them are full-time employees [...]"
~ Respondent 15.

Collaboration with universities, research units, and independent academic experts is gaining increasing importance. Companies are developing these relationships in the form of expert consulting-especially within research and development (R&D) projects-as well as in processes related to product certification and system-level threat analysis. This cooperation brings up-to-date scientific knowledge into organizations, supports innovation, and strengthens their position as competent partners for public and international institutions.

The competencies of company teams are generally rated very highly-especially where teams have been developed organically through a long-term, conscious process of building human capital. Companies that have invested in long-standing relationships with employees and internal educational initiatives (e.g., cybersecurity academies) emphasize strong internal bonds, high trust in team competencies, and alignment in work culture and values.

"For a few years now, we've had a permanent team and honestly, we haven't had time for any active recruitment in this area. So I can't say what's happening on the market, because we have this steady team that fulfills its tasks." ~ Respondent 1.

Additionally, many firms have implemented development programs that serve as a bridge between the academic environment and the labor market. Internal academies and specialized courses for students and young professionals aim to prepare future specialists for real-world conditions in the sector, taking into account its specificity and current needs.

Such programs therefore serve a dual purpose: on the one hand, they provide companies with better-prepared candidates; on the other hand, they strengthen the organization's image as an entity engaged in market development and supportive of education. Some companies offer participants of such initiatives mentorship, access to real-world projects, and the opportunity to gain their first professional experience under the guidance of experts.

Despite the positive evaluation of existing teams and development efforts, respondents pointed to a significant and increasingly noticeable issue-a systemic shortage of qualified specialists in the field of cybersecurity. Staff shortages are evident not only at the national level but also across Europe, particularly affecting the most advanced roles-such as security architects, strategic experts, and individuals who combine high-level technical skills with competencies in sales, management, or communication.

Recruitment Challenges and Workforce Shortages

Most respondents reported no significant recruitment problems in the past year. They highlighted the effectiveness of internal initiatives, strong teams built in earlier years, and cooperation with universities as key strategies for attracting young talent. Nevertheless, even among these companies, some pointed to challenges in hiring professionals for roles that require a combination of diverse competencies-particularly technical and strategic skills.

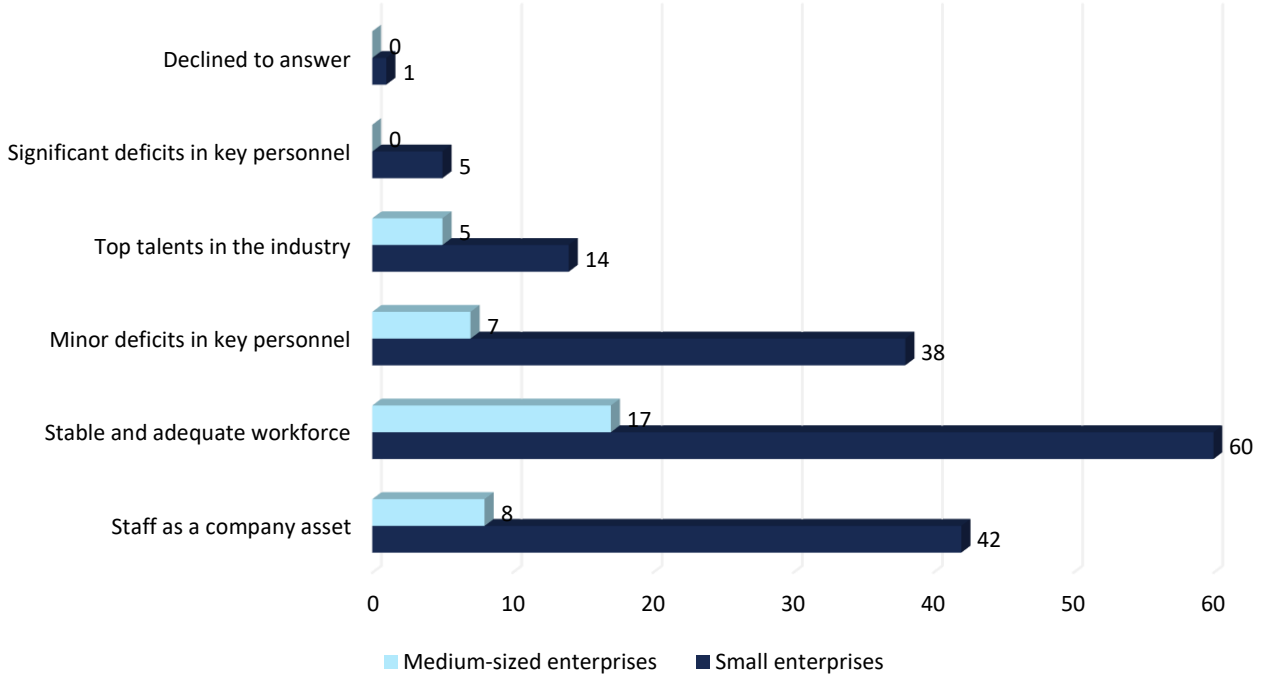
"At the moment, we don't have such problems. We've never really had them. We also work closely with universities. We run various student projects. It's a good way to get to know people who may be more ambitious, talented, and willing to take on more demanding projects."
~ Respondent 15.

"Recruitment used to be a big challenge, for example 3 or 4 years ago, especially during and after the pandemic. […] But the last recruitment we carried out two months ago-we didn't even manage to go through all the CVs."
~ Respondent 9.

While the current recruitment situation in many organizations is relatively stable, the difficulty in sourcing candidates who combine technical expertise with strategic, managerial, or communication skills may pose a significant obstacle to further development and specialization of cybersecurity teams.

Human resources remain one of the key factors determining the effectiveness of cybersecurity efforts. Therefore, respondents were asked to subjectively assess the professional potential of their staff. The responses offer insight into how well companies believe their teams are prepared to meet the challenges facing the sector.

Chart 12. How would you rate the professional potential of your staff? (N=197)



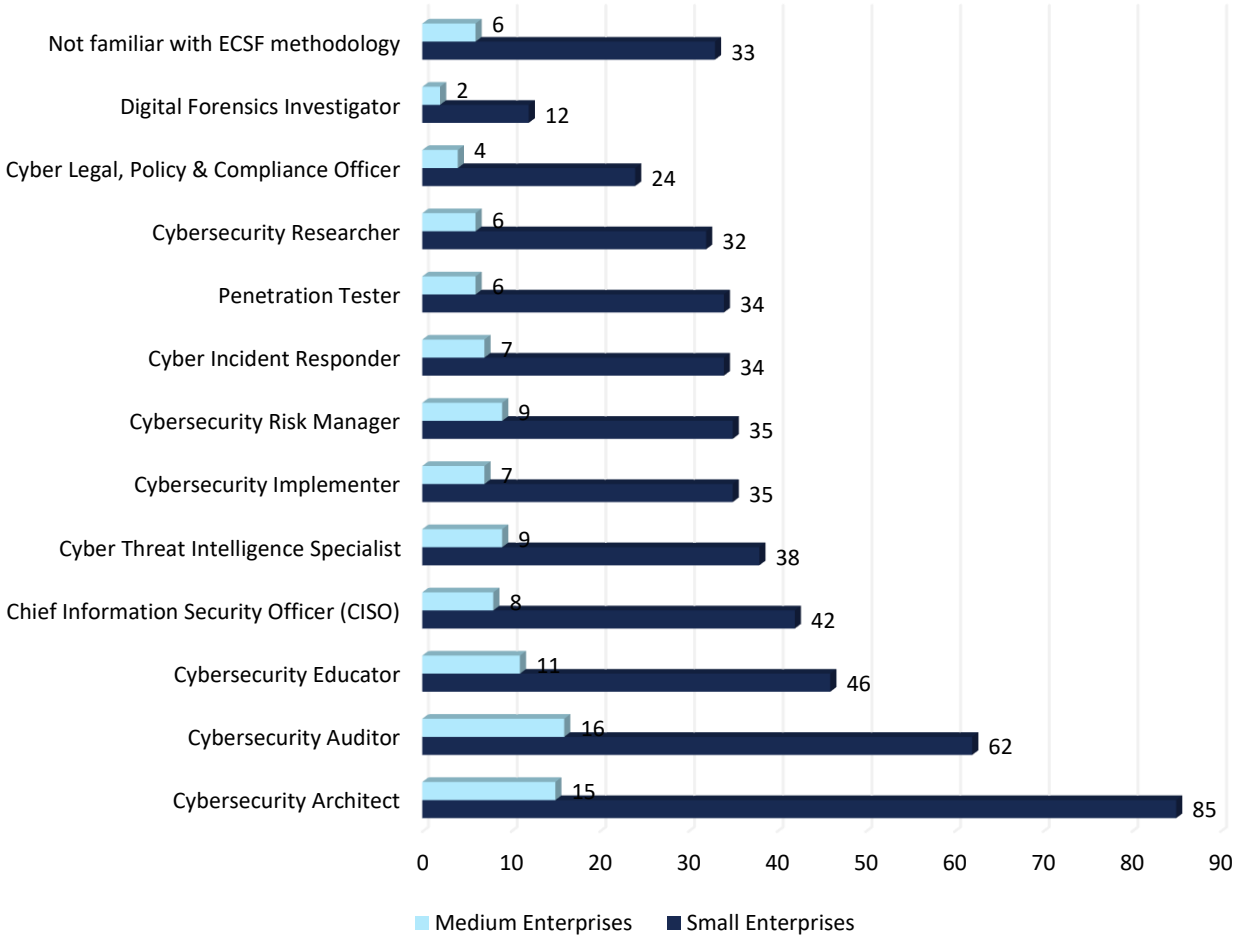
Source: IBC Advisory S.A. analyses based on CAWI survey.

Most respondents expressed a positive assessment of their teams' professional potential. The most frequently chosen response was “a stable workforce adequate to the company’s needs,” selected by 60 small and 17 medium-sized enterprises. A significant number of respondents also stated that their staff is a key strength of the company-an opinion shared by 42 small and 8 medium-sized firms.

The response “minor shortages in key positions” was selected by 38 small and 7 medium-sized enterprises, indicating some, though limited, challenges in recruiting specialists. The highest possible rating, “top talent in the industry,” was declared by 14 small and 5 medium-sized companies, suggesting that only a portion of the surveyed firms view their teams as outstanding in comparison to the competition.

These findings indicate that the vast majority of respondents perceive their teams as sufficiently competent and aligned with the operational needs of their business.

Chart 13. Which roles listed in the European Cybersecurity Skills Framework (ECSF) are present in your company? (N=197)



Source: IBC Advisory S.A. analyses based on CAWI survey.

Among the surveyed companies, the most commonly reported role, according to the European Cybersecurity Skills Framework (ECSF), was that of a Cybersecurity Architect. This role was identified in 85 small firms and 15 medium-sized ones. Other frequently mentioned positions included Cybersecurity Auditor, present in 62 small and 16 medium firms, as well as Cybersecurity Educator, found in 46 small and 11 medium enterprises. The role of Chief Information Security Officer (CISO) was also relatively prevalent, being reported by 42 small and 8 medium firms.

Additionally, roles such as Cyber Threat Intelligence Specialist, Cybersecurity Implementer, Cybersecurity Risk Manager, Cyber Incident Responder, and Penetration Tester were identified with comparable frequency. Each of these roles appeared in 34 to 39 small firms and between 7 and 9 medium firms. In contrast, positions like Cybersecurity Researcher (32 small and 6 medium firms), Cyber Legal, Policy & Compliance Officer (24 small and 4 medium), and Digital Forensics Investigator (only 12 small and 2 medium firms) were less common.

A noteworthy finding is that 39 firms (33 small and 6 medium) declared unfamiliarity with the ECSF framework. This suggests that while the ECSF is gaining visibility, it has not yet achieved widespread recognition across the entire sector.

These results indicate that technical and system architecture-oriented roles are currently the most common in the Polish cybersecurity SME sector. Legal, compliance-related, and digital forensics functions, however, remain underrepresented.

Key Recruitment Challenges: Hybrid and Market-Facing Roles

Among firms that reported recruitment difficulties, the greatest challenges were linked to interdisciplinary "hybrid" roles requiring both deep technical expertise and strong communication, strategic, or business skills. These roles include:

- Security system architects
- Pre-sales leaders and sales consultants
- Technology-business integration experts
- Professionals able to translate tech language into business value

Such competencies have become essential amid digital transformation and the growing role of cybersecurity as a competitive advantage. Organizations aiming to implement and manage complex IT solutions in line with business objectives need professionals who can engage with both technical teams and executive decision-makers.

> *"We're looking for very specific people already vetted by the market. There are great specialists out there, but we need the more universal types-architects or those who can design a process and deliver documentation." ~ Respondent 7.*

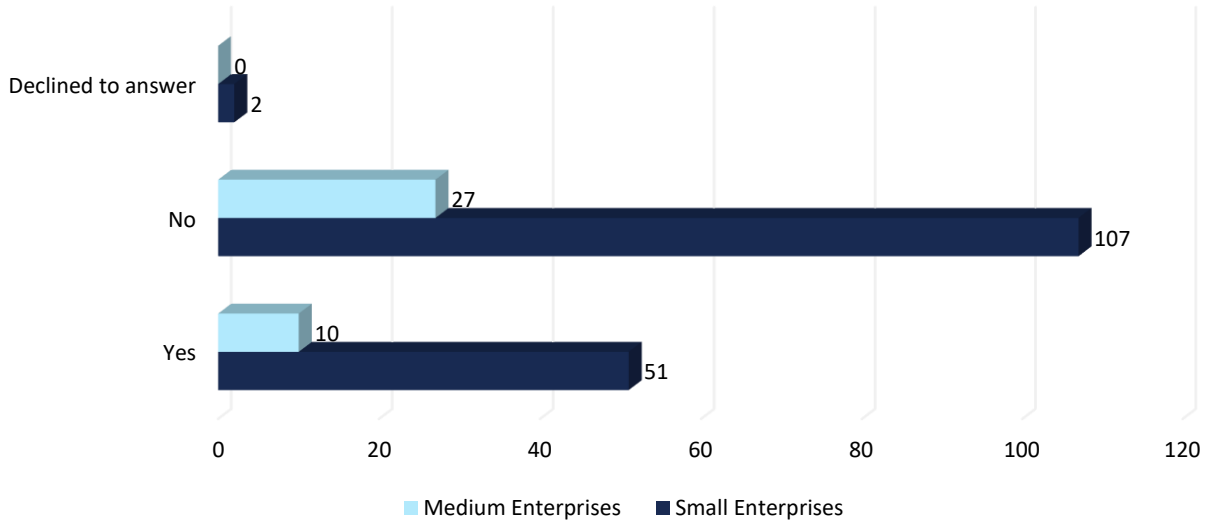
> *"It's really not easy to find people with strong business knowledge in IT. I mean sales leaders, business development, export or marketing professionals-people who can discuss technology in business terms." ~ Respondent 13.*

Smaller companies, despite often offering a more dynamic work environment, struggle to compete for such talent, which may deepen labor market imbalances and hamper the sustainable development of the sector.

Several respondents noted that R&D or engineering teams are not the bottleneck-greater challenges lie in recruiting market-facing roles, such as tech sales experts or client-facing consultants. These positions suffer from high turnover, low motivation retention, and a shortage of candidates with both product knowledge and an understanding of client business needs.

Access to adequately qualified personnel is one of the key factors determining the growth of enterprises in the cybersecurity sector. Therefore, respondents were asked whether they had experienced difficulties in hiring specialists with the required competencies over the past 12 months.

Chart 14. Have you experienced difficulties in hiring adequately qualified employees in the past year? (N=197)



Source: IBC Advisory S.A. analyses based on CAWI survey.

Among the survey respondents, most companies did not experience difficulties in hiring adequately qualified employees in the past year. A total of 107 small and 27 medium-sized enterprises reported no such problems. On the other hand, 51 small and 10 medium-sized firms reported challenges in recruiting suitable specialists. Although these represent a minority, the results indicate that staffing challenges are present in some of the surveyed entities, particularly among smaller companies.
Given the increasing importance of digital security, this finding may serve as a signal to educational institutions, training providers, and labor market policymakers.

Fragmentation of knowledge and specialization complicates the assessment of competencies.

Although cybersecurity is often perceived externally as a single area of expertise, it is in fact a highly diverse and fragmented field, encompassing a wide range of specializations-from technological and infrastructural aspects, through organizational processes, to risk management, auditing, compliance, and crisis communication.
Respondents agreed that expecting "generalist cybersecurity" competencies-i.e., a situation where one expert knows everything-is unrealistic and not reflective of market realities. Each expert develops their knowledge in a specific segment, often highly specialized, due to both the growing complexity of technologies and the pace of changes in the legal and operational environment.

"Cybersecurity is also a very fragmented field, and just because someone says they are familiar with cybersecurity doesn't mean they know everything. Everyone has their own area," ~ Respondent 8.

While many firms report stable recruitment conditions, the market as a whole continues to struggle with a shortage of qualified professionals in selected areas. The labor market is varied-some companies reported no hiring difficulties, while others pointed to specific issues in sourcing both technical and business-oriented specialists.

Team diversity - gender, age, disability

Although gender diversity and inclusivity were not dominant themes in respondents' statements, they emerged as important indicators of growing organizational maturity in parts of the cybersecurity sector. In some cases, respondents explicitly addressed the representation of women in their teams, emphasizing the need to build a work environment based on openness, equal opportunity, and conscious diversity management.

"In my team, I employed 25 people, and I had almost 50% diversity," ~ Respondent 8.

Such a high level of gender diversity in a tech team-particularly in an industry traditionally seen as male-dominated-is a noteworthy example of best practice. It demonstrates that inclusivity can be implemented in practice, not just declared in HR documents. These examples show that, with the right approach, it is possible to create a space where competencies, not gender, determine task assignment and promotion.

Despite some positive examples, the average share of women in tech company structures still ranges from 20% to 40%, with the highest concentration in support departments such as sales, marketing, communications, and customer relations. In these areas, women are not only more visible but also more likely to hold coordinating and managerial roles.

"It kind of split-there are no women in development, but in the sales part, there's (name) for the Polish market, and we have (name) in marketing. Since there aren't many of us overall, we can say the balance is achieved on the business-representative side," ~ Respondent 2.

Women are much less frequently found in strictly engineering, development, or analytical teams, and when they are, it's usually in lower- or mid-level positions. This situation does not stem from a lack of competence but rather from entrenched cultural barriers, a lack of role models, and systemic shortcomings in education and recruitment.

Although women still form a minority in technical departments of cybersecurity companies, there are increasingly visible examples of women holding managerial, architectural, and expert roles. Respondents noted that while development and engineering teams are still male-dominated, in some organizations women hold significant representation at higher levels-

especially where promotions are based on real competencies and experience rather than stereotypical notions of the "typical engineer."

"It's interesting-we've noticed over the years a trend: we have quite a few women. The structure of higher-level positions, like architects or service leaders, is mostly women," ~ Respondent 7.

These are important signals, indicating that real competencies can successfully break gender stereotypes, and that women can thrive in roles requiring both advanced technical knowledge and leadership skills. Such cases challenge the belief that women are "naturally" better suited to supporting functions (e.g., HR, marketing) than hard engineering roles.

From the respondents' statements, it is clear that women's participation in cybersecurity teams largely depends on the specific organization, its operating model, and the local recruitment market. Most firms declare a gender-neutral approach-emphasizing that competencies are the key criterion in recruitment, not gender.

"Yes, we employ women, but unfortunately it's quite a low percentage. Apparently, mostly men applied in the recruitment process, and decisions were made accordingly. We base decisions primarily on the competencies of the person applying," ~ Respondent 10.

However, despite this declared neutrality, most technical teams remain male-dominated. The prevalence of men is not due to overt discrimination or conscious exclusion of women, but rather because women apply less often for technical roles, especially in areas such as software development, systems engineering, or operational security.

Even though women's representation in technical teams remains low in many firms, most of the surveyed organizations report being aware of the need to support diversity and comply with formal equality requirements. This is particularly relevant for companies participating in EU-funded projects, where specific standards apply regarding equality policies, accessibility, and anti-discrimination. Teams often work remotely or in hybrid models, which inherently reduces barriers related to location, mobility, and flexible working hours.

"When implementing any EU project, we must meet all directives related to gender equality, disability, and even rural development. These are required elements, and we meet them 100%," ~ Respondent 3.

In many companies, women hold a variety of roles-from operational to specialist and technical-demonstrating that there are no formal limitations on professional roles, and that real career development opportunities exist regardless of gender.

Wide age diversity-but rarely involving the oldest age groups

Interviews clearly show that individuals over the age of 65 are virtually absent from the structures of companies operating in the cybersecurity sector. In none of the surveyed cases were specialists from this age group reported to be actively employed in technical, operational, or managerial positions. Even in cases where collaboration with seniors was mentioned in the past, it primarily concerned supporting areas such as accounting, HR, administration, or occasional consulting.

The industry remains strongly focused on the professionally active generations (25-55 years), and individuals approaching retirement age-even those with significant experience and expertise-are not considered a target group for recruitment or development activities. The oldest individuals in teams are usually around 60 years old, often in advisory or supervisory roles, with no continuation beyond the 65+ threshold.

"It's a team of very different ages, a wide range. I think the age span is over 30 years between employees […]" ~ Respondent 8.

This could be interpreted as a sign of underused expert potential-particularly in areas such as mentoring, security auditing, systemic risk analysis, or project documentation. In a time of specialist shortages and high demand for institutional knowledge, the professional activation of experienced experts could significantly complement workforce resources. However, this is not currently being put into practice.

The lack of 65+ employees in technical teams is primarily due to the dynamic and demanding nature of the sector. The rapid pace of technological development means that professional experience, while valuable, is often overshadowed by the need

for proficiency in new tools, programming languages, and work methodologies. Despite no formal barriers, older professionals may find it difficult to keep up with the evolving competency requirements of strictly operational roles.

Meanwhile, the presence of people with disabilities in cybersecurity companies remains minimal. In most cases, surveyed organizations currently do not employ such workers. Some respondents acknowledged that in the past, there were isolated cases of employing people with disabilities, but these were not systemic and usually incidental. Only one respondent declared current collaboration with a person with a disability in a technical role:

"[…] we have a disabled person in the development area" ~ Respondent 2.

The data collected suggests that employing people with disabilities in the cybersecurity sector is not part of an actively implemented diversity or inclusion policy. Although some companies report experience in this area, institutional mechanisms to support lasting inclusion are lacking. Particularly underused is the potential of remote and task-based work, which could naturally open up opportunities for people with mobility limitations or the need for a flexible working environment. The absence of such solutions means that despite a declared openness by some firms, opportunities for professional activation of people with disabilities remain largely untapped.

Respondents often pointed out that the nature of tasks performed in companies-including business travel, field work, time and location flexibility, and on-site client presence-may constitute a significant barrier to employing people with disabilities, especially in cases of major physical or health limitations. Many projects require high mobility and direct involvement at the implementation site, which can make it difficult to include employees with specific needs.

"[…] we were considering this perspective. Maybe it's because these projects again require a lot of activity, sometimes also physical, going to the client, and these disabilities […]" ~ Respondent 7.

These statements highlight one of the key challenges of inclusion in the sector-the difficulty of aligning the nature of project-based work with the functional capacities of diverse candidates. In companies operating under task-based models with high operational dynamism and the need for rapid responsiveness, there is a concern that employing individuals with physical limitations may require reorganizing workflows or reducing the pace and quality of execution.

The importance of human capital and skills

Ultimately, even the best technological solutions cannot thrive without the right competencies. Many respondents emphasized that the biggest challenge is not the technology itself, but the lack of people capable of developing, implementing, and maintaining it. Hence, there is a need for investment in education, raising cybersecurity awareness, and creating clear career pathways.

"I believe that cybersecurity competencies can always be improved. […] I think the level of our employees' knowledge has increased" ~ Respondent 10.

These insights clearly indicate that the development of the cybersecurity sector requires strengthening the talent base-both technically and strategically. Without investing in skills, the human potential for innovation will remain underutilized, and companies will be unable to meet the growing demands of the market. It is therefore essential to establish a coherent system for education, career development, and knowledge dissemination that allows for a responsive and skilled workforce.

An analysis of employment structure and staffing challenges in the cybersecurity sector reveals a complex and diverse picture of how firms operate in this space. Enterprises show high organizational flexibility, adapting their collaboration models to changing market and project conditions. Hybrid forms of employment-combining full-time jobs with B2B contracts and project-based cooperation-are commonly used, enabling effective human resource and cost risk management.

Employment scale varies significantly depending on the company's specialization and development stage-from a few to over a hundred collaborators. Even larger organizations often rely on a broad network of external experts and cooperation with universities and the academic community. Stable teams, built on long-term cooperation, are perceived as a key asset-especially regarding loyalty, cultural fit, and high competence levels.

At the same time, despite local stability in some companies, the market as a whole faces a growing shortage of highly qualified specialists. This is particularly true for cross-functional roles-such as system architects, pre-sales leaders, or experts combining technical knowledge with strategic and sales skills. Recruitment difficulties are exacerbated by strong competition from large corporations and tech hubs offering higher salaries and broader development opportunities.

A skills gap is also evident in supporting areas, such as marketing and cybersecurity solution sales. Companies struggle to find individuals who can effectively communicate the value of technology services and translate them into business terms.

Against this backdrop, issues of gender, age, and disability diversity remain largely unresolved. Although awareness of diversity and equal opportunity is growing, actions in this area are mostly declarative. Women's participation in technical teams remains low, and individuals aged 65+ and those with disabilities are rarely present in organizational structures-usually in administrative or support roles. Companies seldom conduct systematic inclusion efforts-there is a lack of tailored recruitment campaigns, adapted workstations, or DEI policies.

In summary, the cybersecurity sector is characterized by high adaptability and organizational awareness but faces structural and systemic challenges. Developing a modern, resilient workforce requires not only strengthening technical skills but also investing in soft skills, diversity and inclusion policies, and close cooperation with the education sector.

2.2. Technological and Infrastructural Potential

The cybersecurity sector in Poland is developing dynamically, shaped by both emerging technologies and geopolitical factors. Based on the conducted qualitative and quantitative research, key trends and needs have been identified that will influence the industry in the coming years.

One of the critical challenges is the prediction phase - anticipating potential threats. While detection and response technologies are becoming increasingly effective, many organizations still lack tools for analyzing risk scenarios. As a result, the importance of threat intelligence and predictive analytics is growing, shifting the focus from reactive to preventive measures.

Another area requiring attention is the security of cloud environments. Distributed IT architectures demand new approaches to identity and access management. IAM (identity & access management) solutions are becoming essential elements for protecting digital assets.

The development of AI-based technologies, including generative AI, brings new risks related to the quality and security of generated code. This creates a need for new audit standards and training for developers in cybersecurity.

In the context of strategic security, Poland gains a competitive edge due to its geographical location and operational experience. Practical knowledge acquired in real threat environments can become an asset in the international arena.

The public sector can act as a catalyst for innovation by becoming a major client and testing ground for domestic solutions. However, investments are needed in both technical and strategic competencies to effectively harness the sector’s potential.

Respondents also emphasize the importance of diversity - especially in terms of women's participation and building inclusive teams. Cultural and skillset diversity can foster innovation and enhance the sector’s resilience to future challenges.

The sector’s development requires systemic action - from education, through legislative and promotional support, to strengthening Poland’s position in foreign markets. Only joint efforts by businesses, government, academia, and industry organizations will allow full utilization of the Polish cybersecurity sector’s potential.

Threat Prediction and Cyber Threat Intelligence (CTI)

According to some experts, the weakest link in protecting organizations from cyber threats is the prediction phase - forecasting potential incidents. While detection (EDR, antivirus) and response technologies are becoming increasingly advanced, few companies have procedures and tools for analyzing possible threat scenarios. This is why there is growing interest in threat intelligence - both in terms of consulting services and solutions that automate the collection, analysis, and correlation of threat data.

"[…] most companies have poorly organized PREDICT phases, meaning very few companies actually carry out prediction of cyber incidents […]" ~ Respondent 7.

These observations indicate that developing competencies and tools in threat prediction is becoming a priority for strengthening digital resilience. A gap at this stage of the security cycle - between threat identification and active mitigation - can lead to delayed responses and increased vulnerability. Therefore, investments in predictive analytics and threat intelligence, along with fostering a culture of foresight based on systematic risk identification and modeling, are necessary to shift from reactive to preventive cybersecurity approaches.

Cloud and Identity Security

One of the most frequently mentioned areas for development is cloud security. Respondents noted that more companies are migrating their systems to cloud environments, but this is not always accompanied by appropriate awareness and control. In particular, they emphasized the need for identity & access management (IAM) tools, which in a distributed environment become a crucial component of security architecture.

"[…] more and more companies are using cloud solutions, and it's not that simple to control everything that's going on in those systems" ~ Respondent 10.

From the respondents' perspective, the effectiveness of security systems in cloud environments will increasingly depend on organizations' ability to manage identity and access dynamically, contextually, and automatically. Distributed IT architecture - typical for modern business models - necessitates a shift from traditional perimeter protection toward user-centric access controls. In this context, IAM solutions are becoming a key integrator of technological, procedural, and organizational aspects. Their development - in terms of both functionality and accessibility for smaller entities - will significantly impact the security of entire digital ecosystems.

Risks Related to Generative Artificial Intelligence

There is also reflection on the risks posed by AI, particularly in the context of source code generation. Concerns were raised that new generations of developers, aided by no-code systems and automated coding tools, may not be able to properly assess the quality and security of the generated code. This creates new risks related to compromised libraries, hidden vulnerabilities, and hard-to-detect errors - especially those generated by the same algorithms.

"[…] it's hard to teach LLMs to catch errors they've created themselves, because it's difficult to test your own mistakes" ~ Respondent 6.

With the rapid development of AI tools, especially generative ones, new challenges arise in ensuring source code security. The risks identified by respondents highlight a gap between the pace of technology adoption and the ability to use it safely. The observed skills gap among younger programmers, supported by no-code platforms and AI, indicates the need for new code auditing standards, quality control mechanisms, and education in secure software development. Without this, the IT sector may face an increasing problem of "black boxes" - solutions created by models whose operation is opaque even to their users.

Cybersecurity in the Geopolitical Context

Respondents frequently indicated that the geopolitical situation - especially the eastern border of Poland and the ongoing war in Ukraine - has a tangible impact on how Polish security solutions are perceived: as particularly relevant and "close to practice." They emphasized that Poland, as a border country, has unique competencies in responding to digital threats, which can be an asset in cooperation with foreign partners and the public sector.

> *"Our product - a system for protection against cyberattacks - is seen by our foreign partners in the context that we, as Poles, understand this" ~ Respondent 2.*

The respondents' statements suggest that Poland's geographic location and direct experience with conflict on its eastern border create unique conditions for cybersecurity competency development. In times of increased geopolitical risk, practical knowledge and operational readiness gain particular significance - which can become a competitive advantage for Polish companies internationally. This potential should be reinforced through systematic support for international cooperation and by promoting Poland as a credible and experienced partner in digital security.

Collaboration with the Public and Defense Sectors

Several respondents expressed the belief that the future of cybersecurity technology development in Poland may be closely tied to growing demand from public institutions, the military, and the national security sector. There are already examples of projects conducted for the Ministry of Defense (MoD), but their number should increase to fully leverage the potential of innovative solutions.

> *"In general, I believe that the state should support technology development so that we, or the EU, are countries that are self-sufficient - and support from the state in this kind of economic and technological development is key" ~ Respondent 7.*

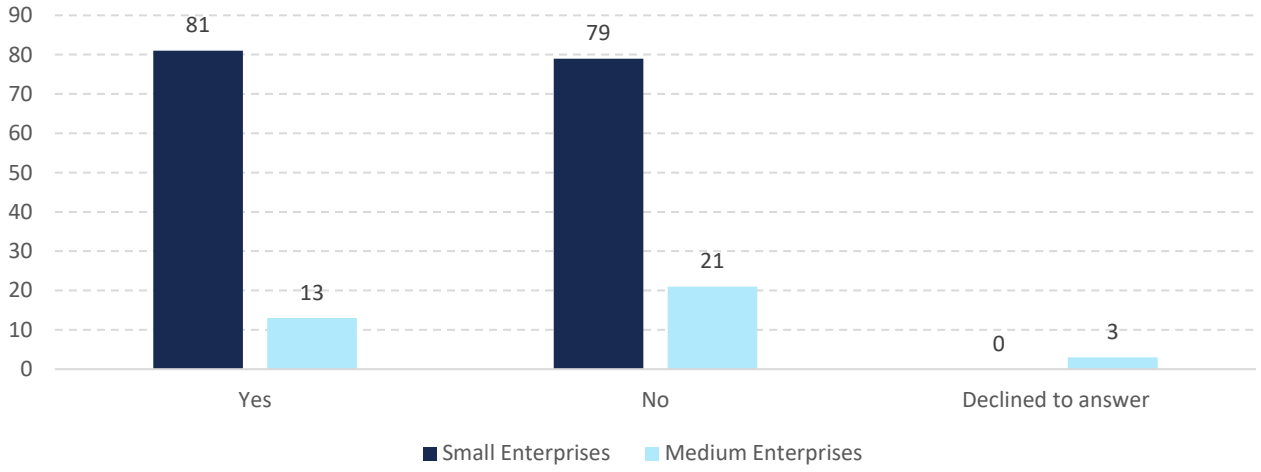
> *"[…] The state sees things from its own perspective, and I think that using our geopolitical position here is a real advantage - plus cooperation with the public sector, including civilians and the military. We already have some interesting examples of projects implemented for the MoD. We just need more of them" ~ Respondent 8.*

These statements confirm that the public sector - including state administration and defense-related institutions - can play a key role as a recipient and promoter of innovative cybersecurity technologies. Increasing the number of implementations in this area will not only provide companies with stable contracts but also create a testing environment for complex solutions. In the long term, this could contribute to building a national ecosystem of competencies and solutions capable of competing with foreign vendors in other strategic digital markets.

Product Development and New Functionalities as an Investment Priority

One of the important elements of the study was to determine investment plans of cybersecurity firms for the upcoming year. The analysis of respondents' answers helps assess the overall investment climate in the industry and identify the level of readiness for technological and business development. In particular, it was verified whether companies plan to allocate funds to new projects, product innovations, infrastructure expansion, or international expansion. Chart below presents the distribution of responses to the question about planned investments, illustrating the current moods and development strategies of companies operating in the Polish cybersecurity market.

Chart 15. Do you plan to make investments in the coming year? (N=197)



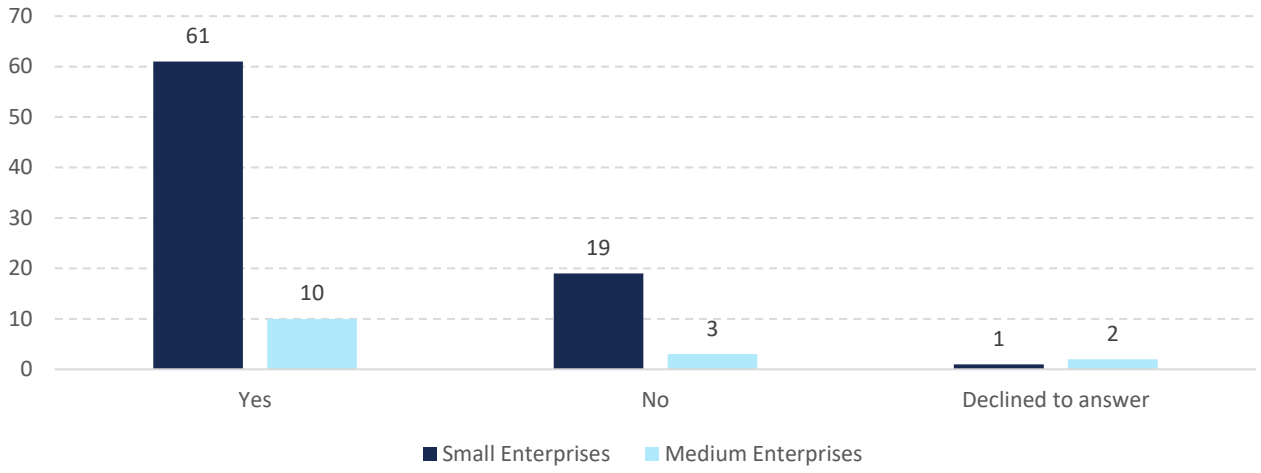
Source: IBC Advisory S.A. analyses based on CAWI survey.

Respondents were asked about their investment plans for the coming year. The responses were almost evenly distributed, especially among small enterprises.
A total of 81 small and 13 medium-sized enterprises declared plans to invest in the upcoming year. Conversely, 79 small and 21 medium-sized companies stated that they had no such plans.

These results indicate a moderate level of investment optimism among respondents - while a significant number of companies intend to grow, an equally large group does not foresee new expenditures in the near future.

Among the companies planning to invest in the next year, particular attention was paid to the purpose of these expenditures. Chart 16 presents the responses to the question of whether planned investments include research and development (R&D) infrastructure. The analysis of this aspect helps better understand the extent to which companies are focusing on creating innovative technological solutions, adapting products to evolving regulations, and implementing automation and artificial intelligence. These data also reveal the dominant investment priorities within the cybersecurity sector and the role that R&D development plays in the growth strategies of these enterprises.

Chart 16. Do the planned investments concern R&D infrastructure? (N=96)



Source: IBC Advisory S.A. analyses based on CAWI survey.

Among the respondents who declared investment plans for the upcoming year (N=99), the vast majority of small enterprises indicated that these investments would focus on research and development (R&D) infrastructure. This response was given by 61 small firms and 10 medium-sized enterprises.
A total of 19 small and 3 medium-sized companies stated that they do not plan R&D-related investments.

Most companies are planning to continue or intensify their research and development efforts, focused on creating modern solutions and updating existing products. Particular emphasis is placed on projects involving service automation using artificial intelligence, the development of authentication mechanisms (e.g. MFA, passwordless login), and compliance with new Europeanlegislation , including the NIS2 directive.

The respondents' statements indicate that these are multi-stage investments, carried out over time and requiring significant input from development and technology teams:

"[…] this year we plan to introduce two complete solutions to the market and also refresh one of our existing devices that has been in use for several years […]" ~ Respondent 1.

"[…] we definitely plan to complete our current investment, which is the third version of the system. As I said, that's 2.5 years of work, an additional team of developers" ~ Respondent 9.

"[…] we are currently trying to build something that I think is a unique service that doesn't really exist on the market yet - an ISAC for small and medium-sized businesses and NGOs […] something that would help them build a foundation for cybersecurity without huge financial outlays […]" ~ Respondent 13.

The new products are expected to be not only technologically innovative but also more affordable and scalable - particularly with the SME segment in mind, which has often been underprotected so far.

Product and Service Portfolio Expansion

Alongside geographic expansion, companies are also developing their offerings - both by creating new products and by adapting existing ones to the specific needs of various markets. Special attention is paid to services and tools compliant with new legislation, such as:

- Multi-factor authentication (MFA),
- Self-service SaaS solutions,
- Threat intelligence sharing platforms (e.g. ISAC for SMEs),
- Products compliant with NIS2, eIDAS 2.0, and DORA.

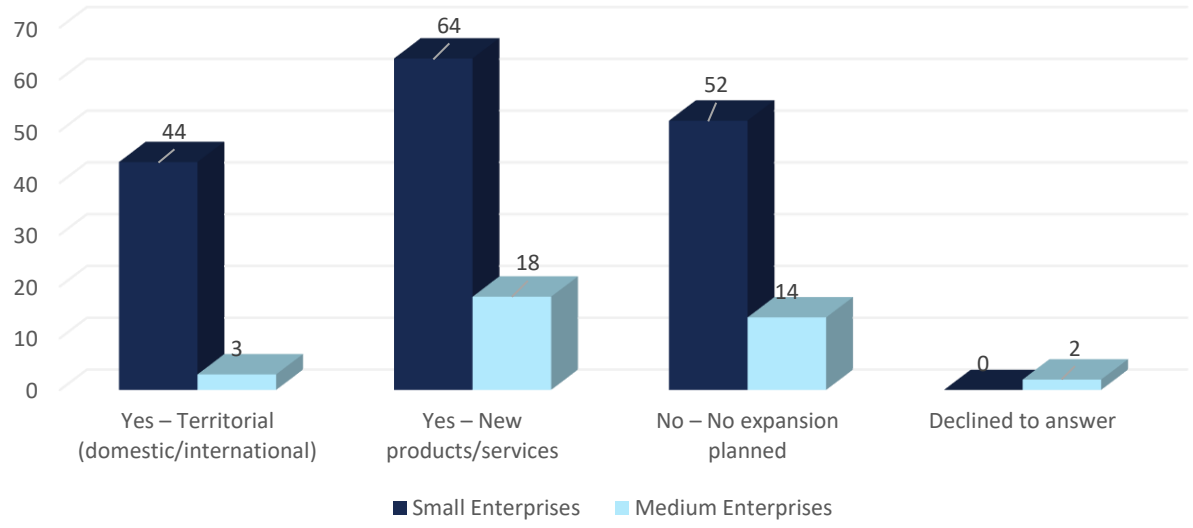
It is worth emphasizing that the strategy to develop the offer does not focus solely on technology. Companies are actively recruiting commercial partners, expanding distribution networks, and building support systems for local clients. Establishing partner channels (partners, resellers, integrators) in different countries is seen as a key component of effective scaling.

"[…] as for distributors, we currently have fifty, but there are many countries and each country may have several distributors, so we are constantly searching for new ones" ~ Respondent 1.

Territorial Expansion: Europe, the Middle East, and North America

The chart below presents cybersecurity firms' expansion plans, both in terms of geography and product development. These results illustrate the market's current approach to growth and scaling, taking into account both development ambitions and limiting factors.

Chart 17. Are you planning to expand your operations? (N=197)



Source: IBC Advisory S.A. analyses based on CAWI survey.

The most frequently declared development direction among respondents was the introduction of new products or services. This answer was selected by 64 small and 18 medium-sized companies. Expansion of operations in territorial terms (domestically or internationally) is planned by 44 small and 3 medium-sized enterprises. Meanwhile, 52 small and 14 medium-sized firms reported having no development plans.

These results indicate that, among the surveyed companies, expanding the product and service offering is the most commonly chosen growth strategy, whereas geographical expansion is considered less frequently-especially among medium-sized enterprises.

Companies plan to expand primarily to European countries-particularly the DACH region (Germany, Austria, Switzerland), Eastern Europe, and countries where advanced cybersecurity regulations are being implemented or are planned. At the same time, bolder plans for expansion beyond Europe are emerging, including to the Middle East and North America.

Company representatives emphasize that interest in their offerings is also coming from international markets, which further encourages concrete steps toward internationalization:

"For now, expansion is definitely focused on Eastern Europe […], but we are also being approached by the Middle East […]" ~ Respondent 4.

In the context of expansion, companies consider not only legal and regulatory issues but also technological aspects. Special attention is given to the location of cloud infrastructure, adaptation of data centers (e.g., in the U.S.), and ensuring compliance with local requirements. All of these efforts require investment, adjustment of sales structures, and reorganization of operations.

Investments in Infrastructure and Team Development

A third strategic investment area is the expansion of technical and human resources. Companies plan to increase employment-mainly in R&D, sales, and marketing departments-as well as invest in physical infrastructure. Examples include building new production spaces, expanding offices, or creating specialized teams to serve new markets.

"[…] we also intend to invest funds in the development of our team and sales and marketing activities in new markets" ~ Respondent 11.

These efforts aim to strengthen the companies' operational capacity and prepare them to serve more clients and projects, both domestically and abroad.

Lack of Active Development Plans - Reasons

Some surveyed companies admitted that, despite being open to occasional development initiatives, their current strategy focuses on key markets considered most important in terms of revenue and stability. The most frequently indicated directions are Western Europe (especially DACH countries) and the United States. These companies deliberately limit the scale of new activities, directing available resources-human, technological, and financial-toward strengthening their position in selected locations.

Statements from company representatives confirm that this approach stems from the need to optimize operations and maximize return on investment:

"We don't currently have any initiatives planned in this area. If a client comes along, of course we can serve them, but our main focus for now is Europe and the United States" ~ Respondent 6.

Another reason for limiting expansion activities is the ongoing nature of current R&D efforts. For many firms, new development directions-both geographic and product-based-depend on the success of ongoing projects. This particularly applies to companies investing in proprietary platforms, security automation solutions, or tools aligned with new regulations.

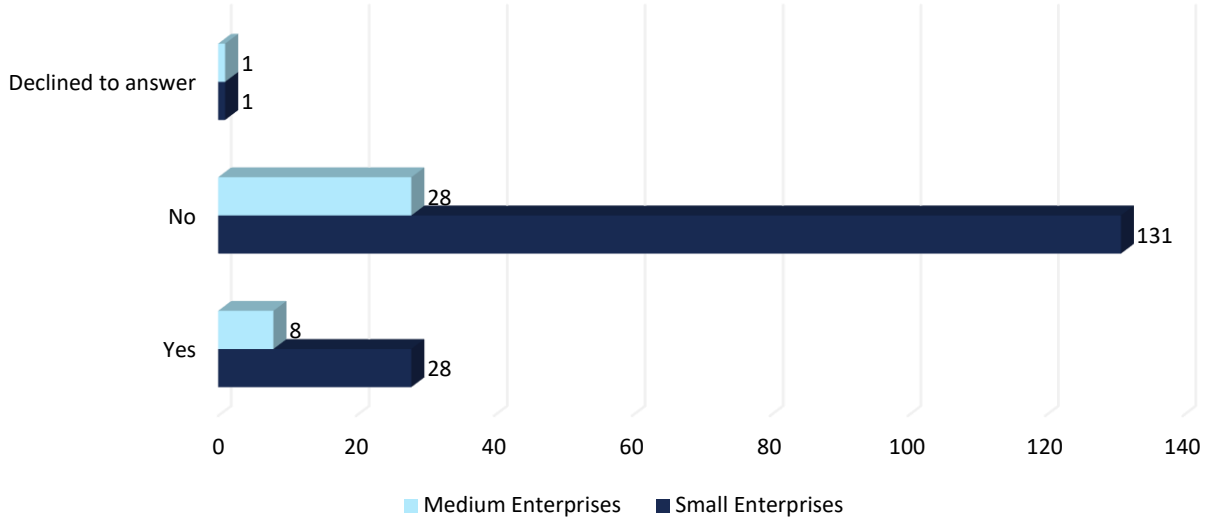
Companies state that strategic decisions will only be made after obtaining measurable results and testing new products in practice:

"[…] we've expanded our platform's capabilities, but we'll wait for the results of the R&D project, which will be in about two years" ~ Respondent 10.

Some companies are still in the planning and analysis stage, considering different development scenarios. Instead of rushing into expansion, they carefully consider implementation models (e.g., internal service development or through a new subsidiary), customer expectations, and potential organizational or reputational impacts. This is especially true for firms considering entry into new service areas such as penetration testing, cloud infrastructure monitoring, or automated security audits..

In the context of supporting innovation and technological development, respondents were asked about their use of technology accelerators or incubators. These institutions play a significant role in accelerating the development of young companies-especially in the tech sector-by offering advisory support, funding, and access to business networks.

Chart 18. Have you used the services of technology accelerators or incubators? (N=197)



Source: IBC Advisory S.A. analyses based on CAWI survey.

Survey respondents were asked whether their companies had used the services of technology accelerators or incubators. The vast majority of both small and medium-sized enterprises reported no such experience. Specifically, 131 small and 28 medium-sized companies responded “no.”

Only 28 small and 8 medium-sized companies reported having used accelerator or incubator services, making them a minority among respondents. These results suggest that although support mechanisms such as accelerators and incubators are available, their uptake among cybersecurity firms remains limited.

The cybersecurity sector in Poland is currently experiencing rapid growth, driven by both technological changes and geopolitical factors such as the war in Ukraine and rising international tensions. A key challenge identified in the sector analysis is the area of threat prediction-anticipating potential incidents before they occur. While many organizations have effective detection and response systems, they lack tools for modeling threat scenarios. Consequently, there is growing demand for advanced threat intelligence and predictive analytics solutions.

Another significant area is the security of cloud environments. As more companies migrate their resources to the cloud, this shift is not always accompanied by adequate awareness and control. Identity and Access Management (IAM) solutions are becoming increasingly important, enabling secure access and identity control in distributed environments. Without proper identity management, even the most advanced security systems may prove inadequate.

At the same time, new threats are emerging from the rise of generative artificial intelligence. Auto-generated code-used by younger developers and no-code platforms-poses risks of hidden vulnerabilities that may be difficult to detect with the very systems that created them. In this context, code auditing, new security standards, and strengthening technical skills are becoming critical.

From a geopolitical perspective, Poland occupies a unique position. As a border country with real-world threat exposure, it has valuable experience that can be leveraged in international partnerships. Respondents highlighted that Poland is perceived as having high cybersecurity competence, which could be a valuable export advantage.

The public sector, military, and national security institutions can act as catalysts for innovation. Increasing the volume of public procurement for domestic cybersecurity solutions would allow companies to develop and test new technologies in

operational conditions. However, this requires investment in strategic and technological competencies within the public administration itself.

Team diversity and inclusion were also indicated as factors that support innovation and resilience against evolving threats. Greater involvement of women and diverse skill sets contribute to the creation of more flexible and effective structures.

To fully harness growth potential, systemic measures are necessary-from educational reform and supportive regulatory frameworks to stronger cooperation between companies, academia, and government institutions. Nearly half of the firms surveyed plan to invest in cybersecurity in the coming year-focusing mainly on product development, service automation, and compliance with EU legislation such as NIS2 and DORA.

Research and development projects are a high priority, including initiatives related to multi-factor authentication (MFA), systems compliant with European regulations, and SaaS services for SMEs. Companies also show interest in international expansion, targeting Eastern Europe, the DACH region, the Middle East, and North America. Key factors in this expansion include compliance with local regulations and availability of cloud infrastructure.

Despite a general sense of investment optimism, firms cite significant growth barriers-primarily overregulation, bureaucracy, and legal unpredictability. New EU regulations require time-consuming contractual and legal adjustments, which strain internal teams and delay product development.

Some companies adopt a more cautious strategy-focusing on core markets and current projects. This approach aims to optimize resource use and maximize investment efficiency. Some firms delay expansion decisions until the completion of ongoing R&D work or the outcomes of pilot projects are known.

Respondents also emphasized the need for strategic planning and adapting business models to customer expectations and local conditions. Rather than rushing, firms aim to carefully assess options, such as service models for cloud infrastructure monitoring or automated security audits.

Lastly, it is worth noting the low use of accelerator and incubator services-81% of companies reported no contact with such institutions. This indicates an underutilized potential of these programs as tools to support innovation in the cybersecurity sector. Promoting and expanding accelerator programs could significantly accelerate the development of young firms and enhance the digital resilience of the economy.

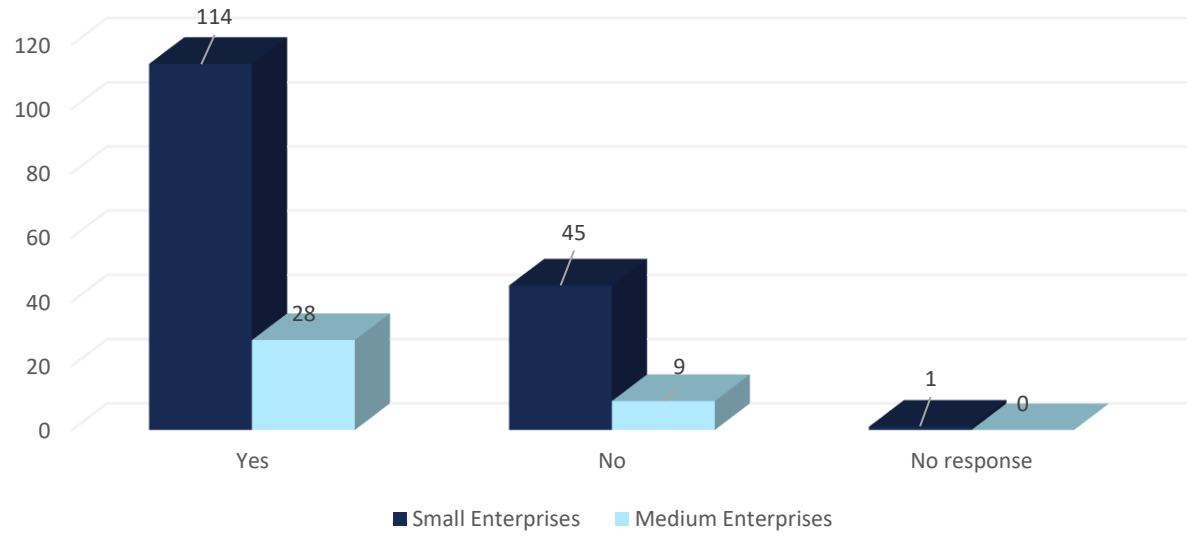
The cybersecurity sector in Poland stands before a significant opportunity for international success-provided there is continued investment, strategic collaboration, and the capacity to swiftly adapt to global technological and regulatory challenges.

2.3. Certification

Certification, intellectual property protection, and compliance with international standards are key elements in building the credibility and competitiveness of companies in the cybersecurity sector—both on the domestic and international markets. In the context of growing regulatory requirements (e.g., NIS2, CRA, DORA) and increasingly high expectations from business partners and public institutions, areas such as certification awareness, readiness to formalize the quality of offered solutions, and approaches to innovation protection are becoming increasingly important.

The following chart presents the level of awareness among companies regarding the certification process, which plays a key role in building customer trust and meeting regulatory requirements in the field of cybersecurity.

Chart 19. Is there knowledge within your company about the certification process? (N=197)



Source: IBC Advisory S.A. analyses based on CAWI survey.

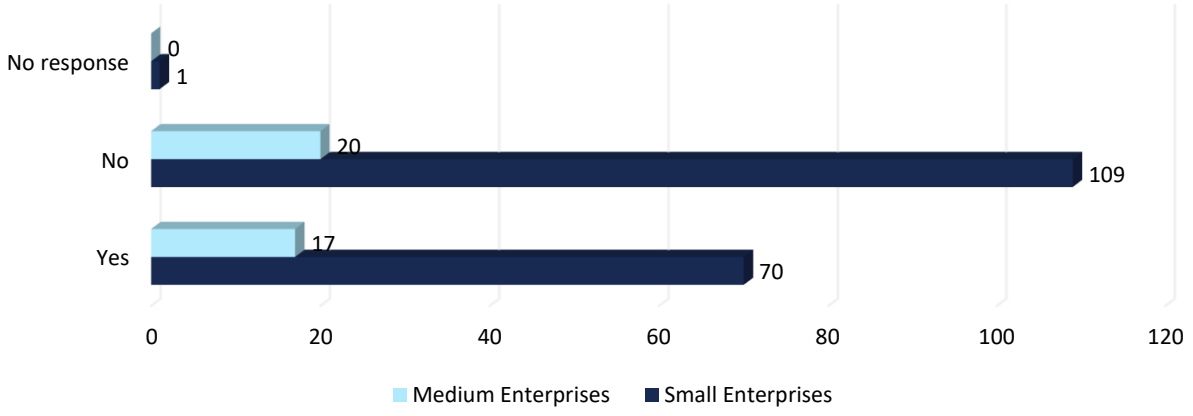
The vast majority of companies - both small and medium-sized - declared that they possess such knowledge. A total of 114 small and 28 medium-sized enterprises responded “yes.”

A lack of knowledge in this area was reported by 45 small and 9 medium-sized firms, indicating that although awareness of certification is high, there is still a group of entities that may require additional informational or educational support.

This result may serve as a trigger for public institutions, chambers of commerce, and industry organizations to carry out informational and training activities that help companies acquire the competencies necessary to initiate the certification process.

The chart below illustrates companies’ approach to the certification of their products and services. These results help assess the market’s readiness to implement formal quality and security standards, which are increasingly becoming a requirement when cooperating with business partners and public institutions.

Chart 20. Do you have plans to certify your products/services? (N=197)



Source: IBC Advisory S.A. analyses based on CAWI survey.

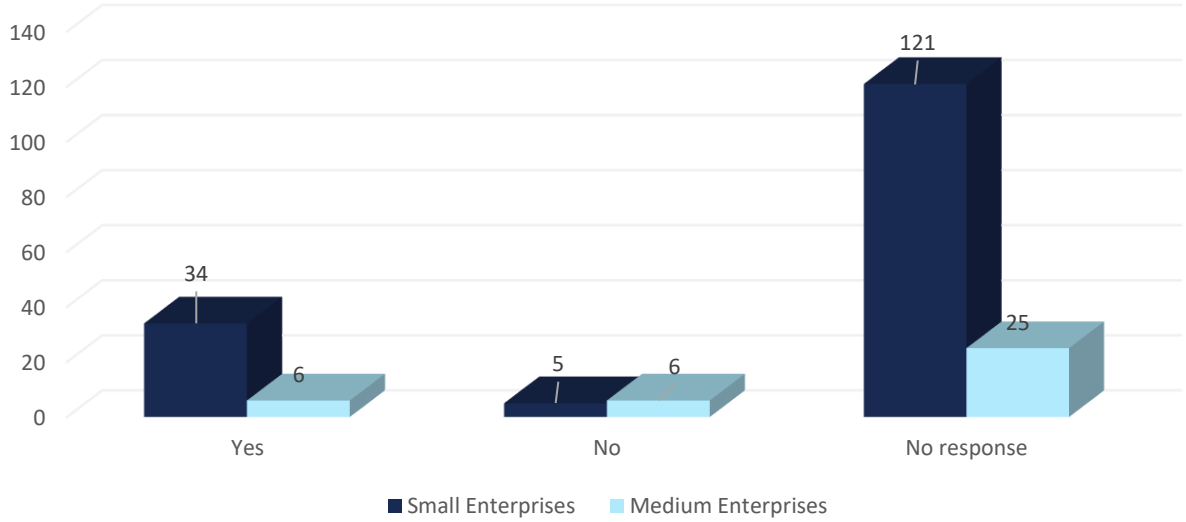
Survey respondents were also asked whether they plan to certify their products or services. The majority of companies - particularly among small enterprises - declared no such plans. This response was given by 109 small and 20 medium-sized firms.

Certification plans were declared by 70 small and 17 medium-sized companies, which represents a significant portion of the sample, although still a minority. This may indicate a growing interest in formally confirming the quality and compliance of offered solutions, especially in light of market and regulatory requirements.

This result points to the existence of a real implementation barrier in the area of standardization and compliance with norms.

The following chart presents the extent to which companies operating in the cybersecurity sector formally protect their intellectual property. The analysis helps assess how widely businesses use legal tools to safeguard innovation and build competitive advantage.

Chart 21. Does your company hold any patents/licenses/trademarks/utility models, etc., related to your products/services? (N=197)



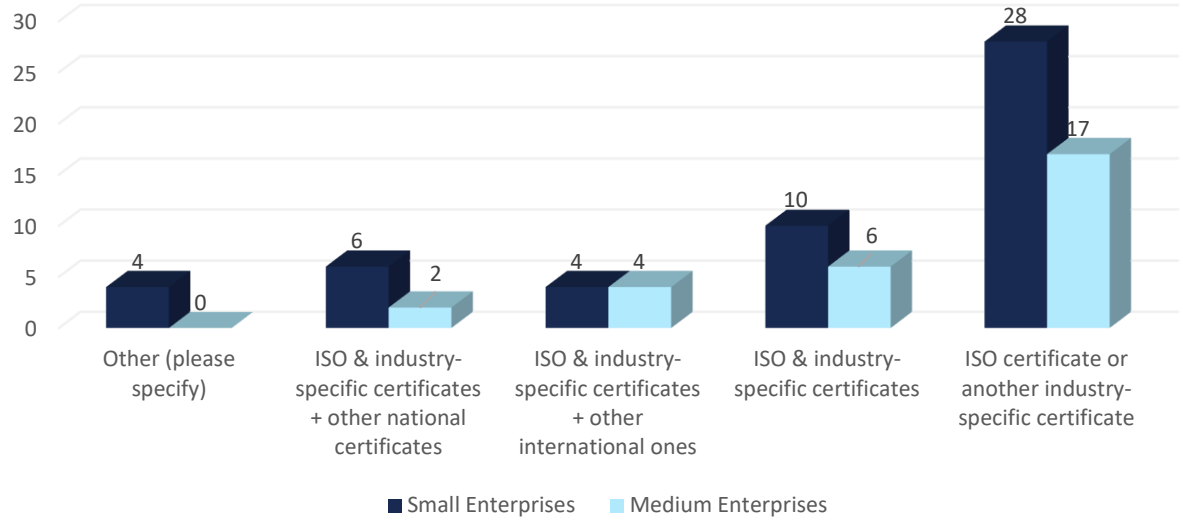
Source: IBC Advisory S.A. analyses based on CAWI survey.

A total of 49 small and 20 medium-sized enterprises declared that they hold such intellectual property rights. In contrast, 108 small and 17 medium-sized companies reported having no formal IP protections in place. This outcome may suggest a limited level of engagement in securing the results of development and innovation activities.

This could stem from both a lack of awareness regarding available mechanisms for intellectual property protection and a relatively low level of innovation or a competitive advantage based on other factors, such as implementation speed or client relationships.

The following chart illustrates which certifications, accreditations, and formal quality documents are held by companies in the cybersecurity sector. These data allow us to identify which standards are most commonly implemented and what approach to formal compliance companies in the sector are adopting.

Chart 22. Number of certifications/accreditations/quality approvals (N=71)



Source: IBC Advisory S.A. analyses based on CAWI survey.

Survey respondents were asked to indicate the types of certifications, accreditations, quality labels, or authorizations held by their enterprises. The most frequently selected answer-among both small and medium-sized companies-was possession of ISO or other industry-specific certifications, indicated by 28 small and 17 medium-sized enterprises.

The next largest group comprised firms holding both ISO and industry-specific certifications-reported by 10 small and 6 medium-sized companies. A smaller number declared possession of ISO and industry-specific certifications along with additional international certifications (4 small and 4 medium enterprises) or national certifications (6 small and 2 medium companies).

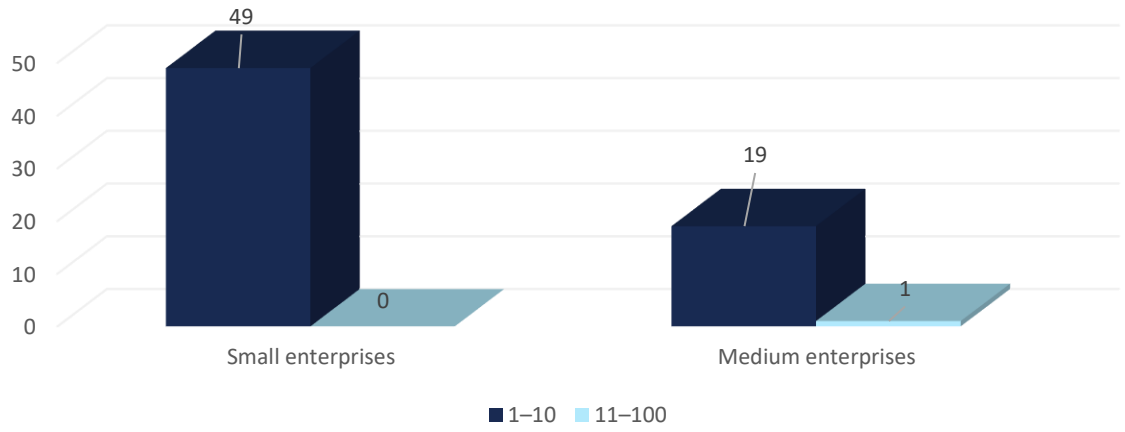
The least commonly selected category included other forms of certification not listed among the main options-marked by only 4 small enterprises, with no responses from medium-sized firms.

These results indicate that certification-particularly ISO and industry-specific standards-is widely adopted among respondents. This may reflect a broader intent to ensure high quality and regulatory compliance in the cybersecurity sector.

Furthermore, while many companies still operate without formal certification, those that do implement such standards tend to focus on internationally recognized frameworks for information security management. This demonstrates an awareness of the importance of standardization and a desire to enhance competitiveness and institutional credibility.

The following chart illustrates the number of intellectual property rights (e.g., patents, licenses, trademarks, utility models) associated with the company's product or service portfolio. These data help assess the extent to which cybersecurity companies formally protect the outcomes of their innovation and development activities.

Chart 23. How many patents/licenses/trademarks/utility models, etc., related to your products/services does your company hold? (N=69)



Source: IBC Advisory S.A. analyses based on CAWI survey.

The majority of companies declared holding between 1 and 10 patents, licenses, trademarks, or utility models related to their products or services. This category included 49 small and 19 medium-sized enterprises.

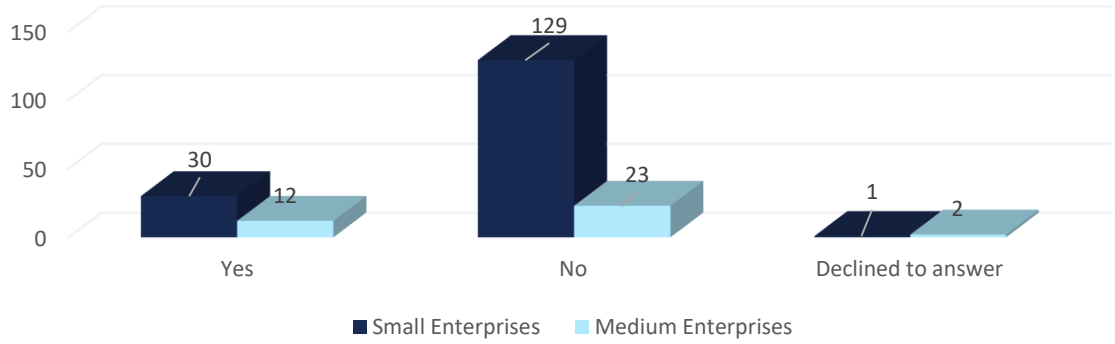
Only one medium-sized company reported owning between 11 and 100 such intellectual property protections, while no small enterprises indicated exceeding the 10-item threshold.

These findings suggest that intellectual property protection is present in the sector, but its scale is generally limited, typically covering only a few solutions per company. This may reflect the early stage of formal IP management practices or a focus on other competitive advantages such as speed to market or client relationships.

2.4. Types of Funding

The chart illustrates whether companies operating in the cybersecurity sector have utilized EU or national funding, with a particular focus on research and development (R&D) projects. The results offer insight into the extent to which enterprises are taking advantage of available instruments that support innovation, technological advancement, and the implementation of new solutions.

Chart 24. Has your company previously used national or EU support to foster development (e.g., R&D projects)? (N=197)



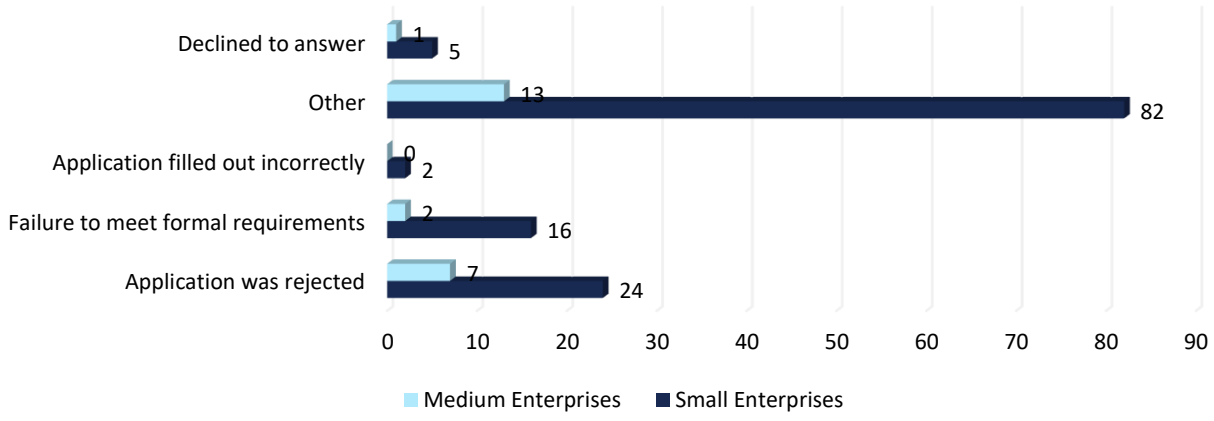
Source: IBC Advisory S.A. analyses based on CAWI survey.

A clear majority of companies reported that they had not used national or EU support to develop their business activities, including research and development (R&D) projects. This response was given by 129 small and 23 medium-sized enterprises. In total, 42 respondents indicated having used public or EU assistance-30 of them small and 12 medium-sized companies.

These results may indicate either limited access to support instruments or a low level of their utilization, especially among smaller entities.

The following chart presents the most commonly cited reasons why companies did not use available national or EU development support, including R&D-related programs. The data include both closed-ended and open-ended responses, providing a broader understanding of the barriers that hinder participation in innovation and technology development support schemes.

Chart 25. What was the reason for not using this type of support (e.g., development or R&D projects)? (N=152)



Source: IBC Advisory S.A. analyses based on CAWI survey.

The most frequently cited reason for not using national or EU development support was categorized as “other, unspecified reasons.” This response was selected by as many as 82 small and 13 medium-sized enterprises. A significant number of companies (24 small and 7 medium-sized) indicated that their applications had been rejected. Another major barrier was failure to meet formal requirements, reported by 16 small and 2 medium-sized firms. There were occasional cases of incorrectly filled-out applications (2 small firms) and refusals to answer (5 small and 1 medium-sized firm).

Among open-ended responses, the most common reason cited was a lack of knowledge about the available programs-their rules, participation requirements, and potential benefits. Respondents repeatedly stated that they were unaware of such forms of support, lacked access to the necessary information, or did not possess the data needed to prepare an application. This lack of basic awareness effectively prevents companies from deciding to participate in development programs and highlights the need for improved communication from institutions offering support.

The second significant barrier was the complexity of application and reporting procedures. Respondents mentioned excessive formality, burdensome documentation, unintuitive rules, and a lack of clear guidance. Some likened the process of securing funding to a lottery, where a single formal error-often beyond the company’s control-could derail the entire effort. These experiences discouraged companies, especially smaller ones, from attempting to apply again.

Another group of responses pointed to a lack of organizational and time resources. Many firms stated that they lacked the staff, time, or internal structure needed to handle a project-from application through implementation to financial reporting. For some respondents, ongoing operational duties left no room for engaging in development activities.

It is also worth noting some respondents expressed a lack of need or motivation to pursue available support. Certain companies admitted they saw no reason to apply for external funding because they had no qualifying projects or felt capable of financing necessary development on their own.

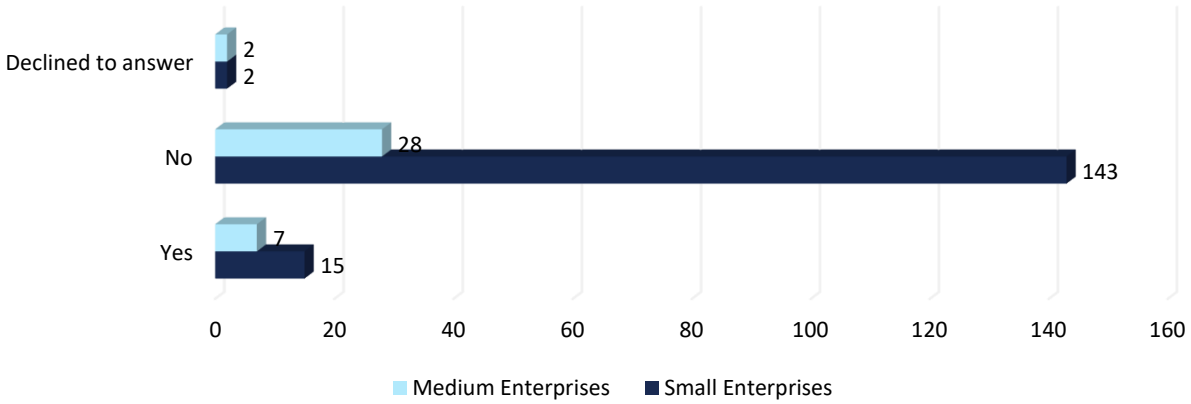
Some respondents expressed distrust toward the support system. Negative experiences-such as application rejections due to procedural issues or problems faced by other companies during audits or reporting-were enough for some firms to completely opt out of seeking funding.

Finally, in a few cases, companies cited ineligibility, such as being classified as a large enterprise or having business activities misaligned with the focus of available programs. These responses demonstrate that not all companies have a real opportunity to benefit from support tools, even when they are aware of them.

Some companies actively obtain EU funds and use them for R&D projects and market expansion

The chart below illustrates to what extent companies in the cybersecurity sector have used available public support instruments-both national and EU-for market expansion purposes. This data helps assess the sector's level of engagement in securing external funding for business growth.

Chart 26. Has the company previously used national or EU support to expand its operations in the cybersecurity sector? (N=197)



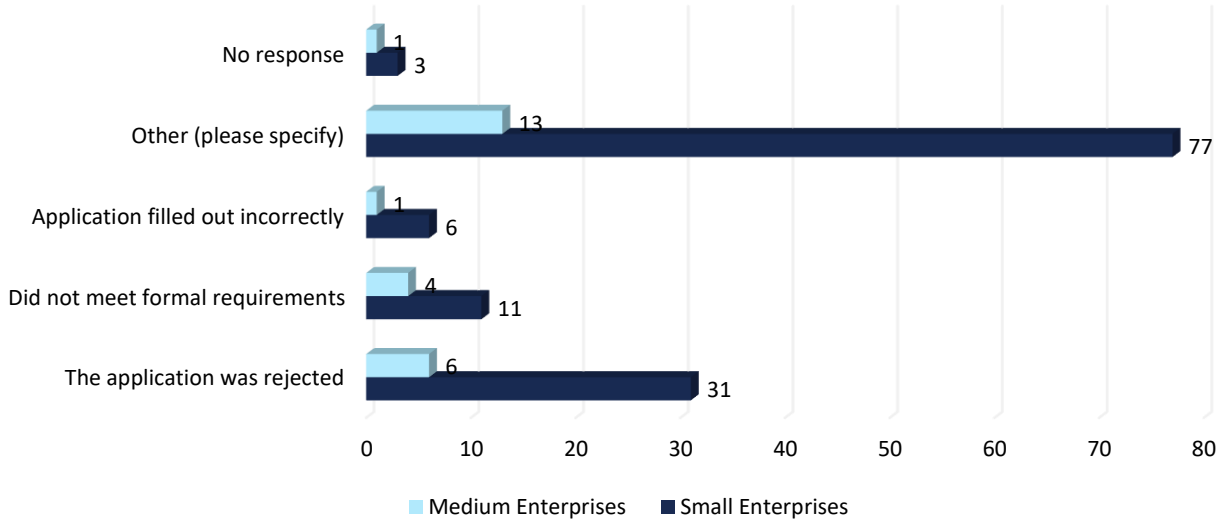
Source: IBC Advisory S.A. analyses based on CAWI survey.

The vast majority of companies have not used national or EU support to expand their operations. This response was given by 143 small and 28 medium-sized enterprises. Only 15 small and 7 medium-sized companies reported having accessed such support.

This low level of engagement with expansion-related funding is an important signal for institutions responsible for designing support instruments. It highlights the need to intensify outreach efforts, simplify procedures, and introduce dedicated mechanisms to foster the growth of companies operating in the cybersecurity sector.

The chart below presents the main reasons why cybersecurity firms did not take advantage of national or EU support for market expansion. The findings are based on both closed and open-ended responses, revealing key barriers such as lack of awareness of available programs, procedural complexity, misalignment of support offers with the specific nature of the business, and internal capacity constraints.

Chart 27. What was the reason for not using this form of support (business expansion)? (N=153)



Source: IBC Advisory S.A. analyses based on CAWI survey.

The most frequently indicated reason for not using national or EU support for expansion purposes was “other, unspecified reasons.” This answer was selected by 77 small and 13 medium-sized enterprises. Among formal barriers, the most common were negative evaluations of submitted applications (31 small and 6 medium-sized firms), as well as failure to meet formal requirements (11 small and 4 medium-sized firms). Occasionally, errors in completing the application documentation were mentioned (6 small and 1 medium-sized enterprise). A total of 4 companies refused to answer. These data indicate that while some companies attempted to obtain support, they often encountered procedural barriers or other difficulties that prevented them from successfully accessing the available instruments.

An analysis of the open-ended responses regarding reasons for not using national or EU support for business expansion highlights several key barriers that limit companies’ activity in this area. The most frequently cited reason was a lack of knowledge about the existence of such programs - respondents stated they were unaware of available opportunities, didn’t know where to look for information, or which support instruments would be appropriate for them. It was also pointed out that the available support was not communicated in a clear and accessible way for SMEs.

The second most common group of responses consisted of statements that the company had never applied - often without giving a specific reason. In many cases, the responses were limited to simple statements such as “we didn’t apply,” “we didn’t use it,” or “we didn’t submit applications.” Occasionally, this was justified by a lack of need, no plans for expansion in that direction, or a focus on current operational activities.

Another significant barrier was the misalignment of the programs with the company's profile or status. Some respondents indicated that the forms of support offered were not suitable for their type of enterprise - for example, larger companies or those operating in specific niches. A lack of projects matching the needs of firms, especially those with an atypical technological profile, was also mentioned.

Some respondents drew attention to the excessive procedural burden, stating that the application process is time-consuming, complicated, and carries a high risk of failure. There were comments that even if a company were interested in support, it lacked the staff or resources to prepare and manage the application effectively. Respondents also pointed to a lack of knowledge about the application process itself, including difficulties in correctly completing the required documentation.

Among the respondents in the in-depth individual interviews, there were also a few strong, ideologically motivated opinions expressing reluctance to use public assistance. Some respondents stated they had no trust in public institutions or perceived support mechanisms as ineffective, unfair, or accessible only to a select few.

Companies with experience in implementing projects with EU funding pointed out the significant impact of such support on the development of R&D infrastructure, capacity building, and scaling their business - including international expansion. Examples included investments in R&D centers and projects worth several million zlotys.

"[…] one of the grants even included the construction of our R&D Center, and we've always been very satisfied; we've never had any issues in that regard. I personally have no complaints about how it works. From various programs," ~ Respondent 1.

"[…] we're currently implementing a project funded by European funds. It started in April. Project value: 4.6 million," ~ Respondent 10.

Some companies are only now planning to apply for funding - previously they didn't have a suitable project profile

These firms have not yet used available support mechanisms, mainly due to a mismatch between their development stage or operating model and the program offerings (e.g., no finished product or a service-dominant offering). However, they expressed interest in ongoing calls and a need for better understanding of the available opportunities.

"No, not so far, because we didn't have a product, and there weren't any programs for services. Now we're thinking about looking for some funding programs," ~ Respondent 7.

There have also been calls for greater support in sales and promotion, rather than direct funding of production processes

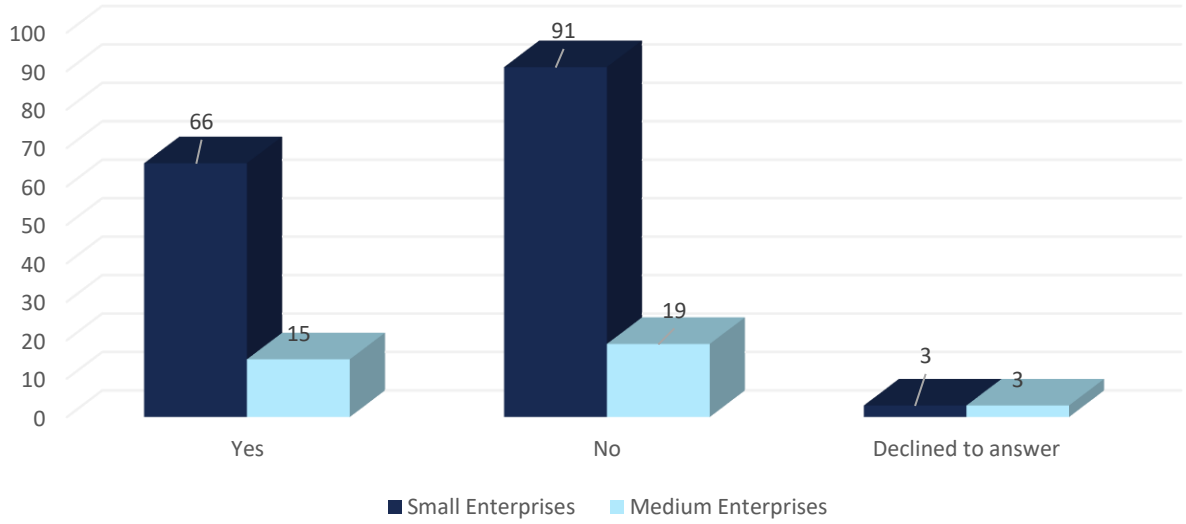
Respondents noted that more developmental impact could come from supporting sales expansion, promotion, and international visibility. There was also a call for better targeting of support - based on the actual commercial potential of products.

"[…] the best source of funding is sales. […] We're heading toward a situation where products are artificially created, and later we'll be wondering why we have such a fantastic product worth PLN 100 million, but no one wants to buy it," ~ Respondent 13.

EU Funding

The chart below presents the level of awareness of EU programs supporting the development of innovative products and services among companies in the cybersecurity sector.

Chart 28. Is your company familiar with EU programs supporting product/service development (e.g., Horizon Europe, FENG, Digital Europe)? (N=197)



Source: IBC Advisory S.A. analyses based on CAWI survey.

A total of 81 companies - including 66 small and 15 medium-sized enterprises - declared awareness of EU programs supporting the development of products and services, such as Horizon Europe, FENG, or Digital Europe. However, the majority of respondents were unfamiliar with these initiatives: 91 small and 19 medium-sized companies answered "no." These results indicate a need to intensify information and education activities regarding available innovation support mechanisms.

Some companies actively use available support programs (e.g., Digital Europe, Horizon Europe), treating them as an important source of co-financing for R&D and product development projects. Even partial funding allows them to scale their investments more quickly and build technological advantage.

> *"If we don't have the means to carry out a project with our own resources, because company funds are insufficient, then obtaining financing of even 20-50% makes it possible. […] Even if we had the ability to implement a project worth 100% of its value, receiving 50% in co-financing gives us a handicap to carry out a second project - because the own contribution now covers 50% of two projects, which enables us to implement our plans faster," ~ Respondent 3.*

Procedural difficulties and limited trust in the application review system

Some respondents pointed to formal barriers and low transparency of the application process as discouraging factors. They criticized the complexity of the documentation, long waiting times for fund disbursement, and - in a few cases - doubts about the fairness of the application evaluations.

> *"[…] When it comes to financial support, strictly speaking, I haven't applied for those programs […] I don't really trust how they are assessed, I have very low trust in the evaluation process, very low. […] In general, I don't believe it's fair, and I don't know if it would even be worth the time, because I rate the probability of success as very low - though maybe I'm wrong, I don't know," ~ Respondent 8.*

Need for better coordination and promotion of initiatives at the central level

Some companies signaled limited effectiveness in cooperation with European coordinating bodies (e.g., ECCC) and insufficient promotional support for funded projects. The absence of funding institutions' representatives at industry events limits visibility and the scaling potential of the projects.

> *"[…] there's a lack of promotional support for these projects […] if the EU is already allocating millions of euros for these projects, then it should be interested in promoting them as widely as possible, and in reality, cooperation at that level is practically nonexistent," ~ Respondent 14.*

Most companies avoid private funding due to control concerns and misalignment of goals

A significant portion of respondents stated they had not used VC/PE funding, despite being aware of such opportunities. Key barriers included reluctance to give up equity, a belief that external funds undervalue their company, and a mismatch between cybersecurity sector specifics and investors' expectations.

> *"We didn't want to give up shares, and we thought our internal valuation would likely be higher than the valuation from an external fund," ~ Respondent 10.*

> *"[…] Cybersecurity is also about trust - customer trust in the product and brand. And you can't build that in a week, or a year, or even two. […] The venture market nowadays promotes itself as a force supporting the development of cybersecurity firms - but that's just their marketing," ~ Respondent 9.*

Collaboration with funds is sometimes considered - but with great caution

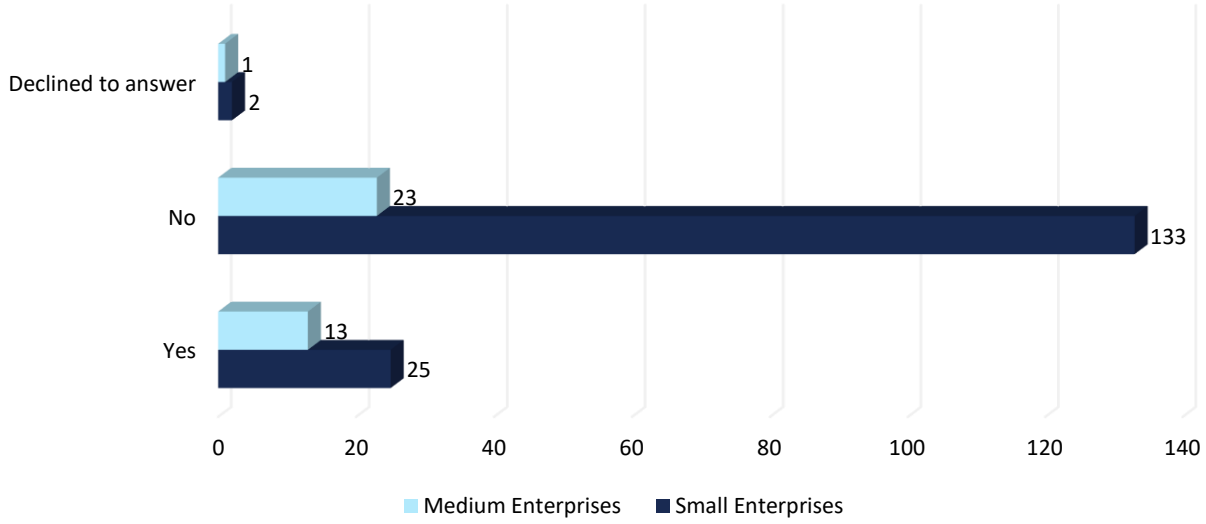
In some cases, companies engaged in talks with investment funds but did not proceed - usually due to overly invasive terms (e.g., requiring majority ownership) or doubts about the added value beyond capital. Many respondents believed that support should go beyond funding - for example, including genuine help with internationalization or strategic planning.

> *"[…] we received several offers for co-financing our activities, but they always came with the condition of taking over the majority of the company - and we didn't agree to that. As I said, we're not just interested in capital," ~ Respondent 2.*

Only a few companies used private financing - mainly in the PE model

The chart below presents the extent to which cybersecurity companies have used private financing over the past three years. The analysis shows to what degree enterprises have sought or obtained support from private investors, such as venture capital or private equity funds.

Chart *29.* Has your company received support from private financing sources (e.g., venture capital, private equity) in the past 3 years? (N=197)

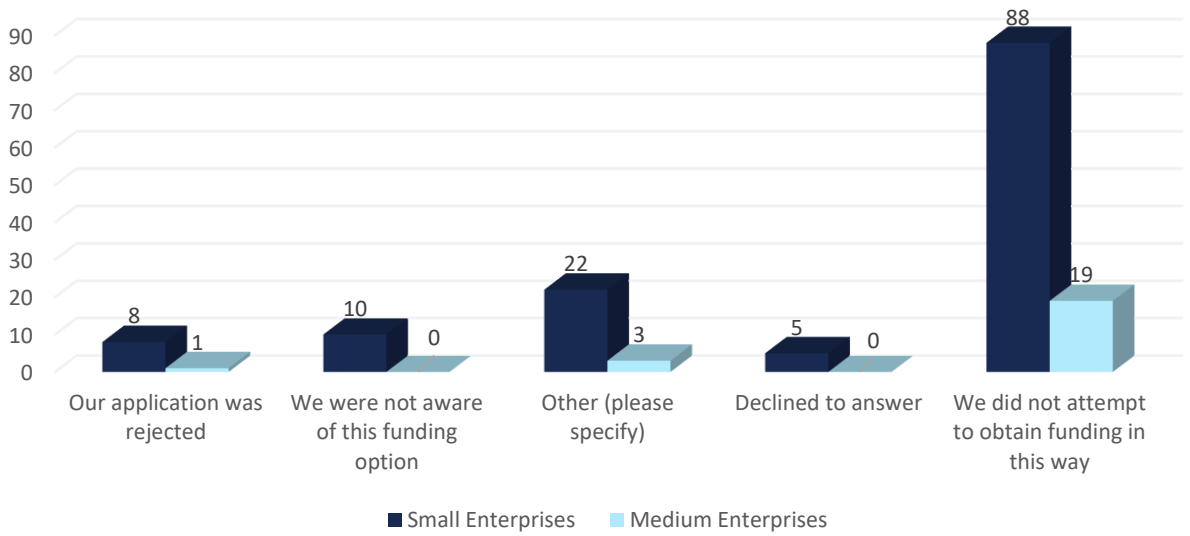


Source: IBC Advisory S.A. analyses based on CAWI survey.

The vast majority of companies have not used private sources of funding-such as venture capital or private equity - over the past three years. A total of 133 small and 23 medium-sized enterprises reported not receiving such support. Only 38 companies- 25 small and 13 medium-sized - obtained private external financing. These figures indicate that although access to private capital is available, it remains a relatively uncommon form of business development support.

The chart below presents the reasons why companies did not seek this type of financing.

Chart 30. If not, what was the reason? (N=156)



Source: IBC Advisory S.A. analyses based on CAWI survey.

The most common reason for not using private forms of financing, such as venture capital or private equity, was the lack of attempts to obtain such support. This answer was indicated by as many as 88 small and 19 medium-sized enterprises. Another significant barrier was the lack of awareness of such a possibility - cited by 10 small firms. Some respondents pointed to other reasons (22 small and 3 medium-sized companies), and a total of 9 firms (8 small and 1 medium) reported that their application had been rejected. These data suggest that the main obstacle to using private financing is not negative experience, but rather a lack of initiative or knowledge about available opportunities.

Based on the analysis of open-ended responses regarding the reasons for not using private financing (e.g. venture capital, private equity), several main categories of reasons can be distinguished. However, most statements were brief, included refusals to answer, or lacked detailed justification.

The most frequently cited reason was reluctance or a lack of need to seek external capital. Respondents wrote directly: "lack of interest," "not interested," "we didn't really need it," or "we use our own funds." Such statements suggest that some companies consciously choose self-financing, not perceiving investor involvement as a necessary or desirable part of development. This may result from a comfortable financial position, a preference for ownership independence, or a lack of belief in the added value of working with investors.

Some responses also pointed to risk and negotiation barriers, e.g., "too much risk" or "no agreement at the early negotiation stage." These answers indicate that even when companies considered cooperation with an investor, the process might have failed due to mismatched expectations or concerns about the consequences. One respondent noted: "the nature of cyber products (dual-use) requires caution when raising capital," suggesting that some cybersecurity firms limit external investor access due to the sensitive nature of their business.

In other cases, general statements were given ("we didn't use that form of financing") or the respondent refused to answer - which occurred in the vast majority of cases. This may indicate reluctance to disclose motivations, lack of reflection on the subject, or the marginal role of this financing form in the companies' strategies.

A few cases pointed to the use of private equity - primarily from experienced industry investors. However, these were exceptions rather than a prevailing trend. This indicates a selective approach to such financing and highlights the need to build greater trust between investors and cybersecurity firms.

"Yes, Private Equity mainly, because Warsaw Equity Group is private capital." ~ Respondent 6.

Summary

The collected findings point to an urgent need to simplify application procedures, improve communication around support programs, and better tailor financial instruments to the realities and needs of firms in the sector. There is also a need to promote a culture of innovation, cooperation with investors, and greater trust in public and private funding mechanisms.

The main funding programs used by Polish firms in the cybersecurity industry are mostly focused on R&D projects. This is due to the high capital intensity required to develop a product up to the MVP (Minimum Viable Product) stage, capable of competing in the market. Other funds are mainly acquired through consortia creating joint projects or delivering specific market value for clients.

Public funding programs used by Polish cybersecurity SMEs include:

CyberSecIdent - a dedicated program aimed at increasing cybersecurity in Poland through the development of hardware and software solutions. The project's objective was to advance new technological and methodological solutions in the following areas:

- detection, presentation, and protection against cyber threats and their consequences at the national level,
- digital identity solutions, with consideration of privacy aspects,

- methodologies, techniques, and processes in the field of cybersecurity analysis and digital identity, as well as their implementation.

The program had a total budget of PLN 234,027,000. Eligible applicants were scientific consortia as defined in the Act on the Principles of Financing Science (April 30, 2010)[25]. Funding was allocated across four calls from 2017-2020, and monitoring and evaluation are set to continue through 2030[26]. During the program, 23 projects were funded[27].

Fast Track - digital innovation. Funds from the Fast Track program could be used for industrial research, development work (mandatory), and pre-implementation work[28]. The program's total budget amounted to PLN 811,301,837.90. Eight cybersecurity-related projects were funded under this scheme with a total grant value of PLN 42,460,140.93 (total project value: PLN 61,653,829.34).

European Funds for Digital Development 2021-2027 (FERC) - one of the key financial instruments supporting Poland's digital transformation. The program focuses on developing modern digital infrastructure, strengthening resilience to cyber threats, and increasing cybersecurity competencies in both the public and private sectors[29]. FERC-funded projects included national security systems, data protection tools, and real-time cyber threat detection and response platforms.

European Digital Innovation HUBs - a program supporting the creation of regional hubs for digital transformation to increase the global competitiveness of SMEs by helping them implement the latest digital solutions. Half of the EDIH funding comes from European Funds (DEP), and the other half from national funds (FENG). In Poland, four EDIHs offering cybersecurity services have been established (in one case, the hub is fully focused on cybersecurity):

- **EDIH - Silesia Smart Systems** - Total project value: PLN 21,424,118.47; EU funding: PLN 10,165,502.54. One of the seven partners offers cybersecurity services[30].
- **EDIH - Cybersec EDIH - Silesia Smart Systems** - Total project value: PLN 21,424,118.47; EU funding: PLN 10,165,502.54. One of the seven partners offers cybersecurity services.
- **EDIH - Smart Secure Cities** - Total project value: PLN 11,675,329.68; EU funding: PLN 5,569,261.20. One of ten partners offers cybersecurity services.
- **EDIH - WRO4digITal** - Total project value: EUR 5,055,491.06; EU funding: EUR 2,527,745.49. Four of twenty-two partners provide cybersecurity services.

Cybersecurity firms have also benefited from grants under Regional Operational Programs focused mainly on R&D activities. Examples include:

- **Digital Core Design**, which obtained funding from the Silesian Voivodeship ROP for the project "QBASS - Quantum-resistant Block-based Asymmetric Encryption and Authorization System"[31].
- **Perceptus**, which received funds under the Lubuskie 2020 ROP for the project "Development of a Secure Managed Password Manager"[32].

Despite the availability of various funding schemes, not all Polish cybersecurity firms take advantage of this support effectively. Reasons include a lack of knowledge about financing opportunities, complex application procedures, and administrative requirements for obtaining funding. Additionally, SMEs in particular face organizational and expert resource shortages that make it harder for them to compete with larger entities for funds.

Going forward, the further development of digitalization and cybersecurity support programs should include the simplification of application procedures and better information and advisory services for companies. This could increase the

[25] Założenia programu B+R CyberSecIdent: Cyberbezpieczeństwo i eTożsamość, aktualizacja nr 4, s. 34. Narodowe Centrum Badań i Rozwoju. [Access: 11.04.2025]
[26] Ibidem., s. 40-41.
[27] Raport "Polski rynek cyberbezpieczeństwa 2023–2028". Polski Klaster Cyberbezpieczeństwa #CyberMadeInPoland, Październik. 2023, s. 113.
[28] Artykuł "Szybka ścieżka – Innowacje cyfrowe (1/1.1.1/2022)." Narodowe Centrum Badań i Rozwoju. [Access: 11.04.2025]
[29] Informacja o programie Fundusze Europejskie na Rozwój Cyfrowy 2021-2027. [Access: 18.04.2025]
[30] "Artykuł "O SIlesia Smart Systems", Silesia Smart Systems. [Access: 17.04. 2025]
[31] Informacja o firmie "DCD. Company. R&D", DCD, 2025. [Access: 18.04.2025]
[32] Informacja o firmie "Perceptus. Projekty Unijne", Perceptus, 2025.[Access: 18.04.2025]

uptake of available funds, contributing to the dynamic growth of the Polish cybersecurity sector and enhancing its international competitiveness.

Looking at the value of grants applied for by cybersecurity firms under R&D programs, it can be assumed that the optimal range is between PLN 1 million and 10 million (excluding the own contribution required by the specific call).

Private Funding for Growth

Private funding for Polish cybersecurity companies has been steadily increasing, enabling more dynamic business development and international expansion. Notable examples of firms that have secured private funding include:

1. **Sagenso (formerly CyberStudio)** - In 2021, Status Starter VC invested PLN 2 million to support the company's further development[33].
2. **ICsec** - In 2022, ICsec received funding from an investment fund owned by PKN Orlen. ORLEN VC independently subscribed to the company's share issuance. The investment amount was not disclosed[34].
3. **Secfense** - In 2022, Secfense raised USD 2 million in a funding round involving VC funds from Estonia, the Czech Republic, Poland, and individual investors such as Tera Ventures, Presto Ventures, RKKVC, and business angels[35].
4. **Resquant** - In 2023, Invento VC invested PLN 1.1 million in ResQuant for organizational development[36].
5. **Authologic** - In 2024, YCombinator, Peak Capital, and SMOK VC jointly invested USD 8.2 million in Authologic to support the company's international expansion[37].
6. **Xopero Software** - In 2024, Warsaw Equity Group invested PLN 20 million (with the option to extend to PLN 30 million) in Xopero Software to accelerate its international growth[38].
7. **Fudo Security** - At the beginning of 2025, bValue invested PLN 40 million in Fudo Security to support its dynamic development, especially in the U.S. market[39].
8. **CyCommSec** - The company attracted investors in 2025, though the investment amount was not disclosed[40].

Investment announcements clearly show that investors favor companies ready to scale internationally. Such readiness often stems from prior R&D grants that help develop competitive products.

There have also been several acquisitions of Polish cybersecurity companies:

1. **ComCERT** - In 2019, Asseco Poland acquired 69.01% of ComCERT shares, becoming its majority owner[41].
2. **Famoc** - In 2021, Techstep acquired 100% of Famoc's shares for approx. PLN 47 million[42].
3. **Digital Fingerprints** - In 2022, the Credit Information Bureau (BIK) added Digital Fingerprints to its portfolio through an agreement with previous investor mAkcelerator. The transaction value was undisclosed[43].
4. **Cryptomage** - In 2023, Atende acquired 20% of Cryptomage shares, with plans to increase its stake to 31.63% by buying out Starfinder Capital[44].

Role of Industry Incubators and Accelerators in Driving Innovation and Competitiveness

Incubators and accelerators play a key role in the innovation ecosystem by supporting startups and young companies in the cybersecurity sector. One example is the **Krakow Technology Park**, which, in cooperation with AGH University, runs the Polish branch of defence innovation accelerator NATO- DIANA call **Fort Cracow**. This initiative aims to align the capabilities of scientists, innovators, and startups with the needs of the defense and military sectors. It is complemented by the launch

[33] Artykuł w portalu branżowym "Satus Starter VC zainwestował 2 miliony zł w Cybersecurity Studio". MamStartup, 2021. [Access: 18.04.2025]
[34] Artykuł „ORLEN VC z pierwszą polską inwestycją bezpośrednią." PKN ORLEN, 2022. [Access: 18.04.2025]
[35] Artykuł „Secfense pozyskuje 2 miliony dolarów w kolejnej rundzie inwestycyjnej." Secfense, 2022. [Access: 18.04.2025]
[36] Artykuł w portalu branżowym „ResQuant z branży cybersecurity pozyskał finansowanie od Invento VC." MamStartup, 2023. [Access: 18.04.2025]
[37] Artykuł w portalu branżowym „Authologic z pomocą SMOK VC pozyskuje 8,2 mln dolarów na rozwój globalnej platformy weryfikacji tożsamości cyfrowej." MyCompany Polska, 2022. [Access: 18.04.2025]
[38] Artykuł w portalu branżowym „Inwestycja 20 mln zł w Xopero." CRN, 2024. [Access: 18.04.2025]
[39] Artykuł w portalu branżowym „40 mln zł na cyberbezpieczeństwo od bValue. Fudo Security rozwinie skrzydła w USA." XYZ, 2025. [Access: 18.04.2025]
[40] Wpis na stronie kancelarii prawnej „We advised CyCommSec." LLW Lewczuk Łyszczarek Szymczyk, 2025. [Access: 18.04.2025]
[41] Wpis w portalu branżowym „Asseco Poland kupiło 69,01% akcji spółki ComCERT." Money.pl, 2019. [Access: 18.04.2025]
[42] Strona internetowa firmy „Techstep acquires software company Famoc, adding MMS capabilities." Techstep, 10 maja 2021. [Access: 18.04.2025]
[43] Artykuł w portalu branżowym „Biuro Informacji Kredytowej inwestuje w polski fintech Digital Fingerprints." MamStartup, 2022. [Access: 18.04.2025]
[44] Strona internetowa firmy „Atende inwestuje w Cryptomage – spółkę łączącą AI z cyberbezpieczeństwem sieciowym." Atende, 2023. [Access: 18.04.2025]

of **NATO's Innovation Fund (NIF)** - the world's first multinational venture capital fund - supporting innovation in emerging and disruptive technologies (EDTs) such as AI, autonomy, space tech, hypersonics, quantum computing, and next-generation communication networks[45].

The **Polish Agency for Enterprise Development (PARP)** has launched programs such as *Startup Booster Poland - Smart UP* to support new accelerators in scaling and commercializing innovative solutions. The latest call under the *European Funds for a Modern Economy (FENG)* program selected 17 winning projects with a total budget exceeding PLN 260 million. These projects offer acceleration and post-acceleration services[46].

According to the **Dealroom CEE 2025** report, further efforts are needed to support international expansion and develop "soft-landing hubs" that assist startups in entering strategic markets such as the U.S., the U.K., and Germany. Recommendations also include investing in emerging startup ecosystems in cities like Wrocław, Poznań, and Gdańsk, alongside established hubs like Warsaw and Kraków. Infrastructure investment is also crucial - coworking spaces, incubators, mentoring programs, and dedicated accelerators for defense and cybersecurity. Cooperation between startups, NATO, and the public sector could open new funding channels and accelerate innovation adoption. Investment funds focused on security-related technologies could further enhance Poland's leadership position in this area[47].

Engagement with incubators and accelerators not only supports technological growth but also builds Polish cybersecurity firms' capacity in management, marketing, and foreign expansion - significantly increasing their competitiveness.

2.5. Internationalization of Companies

One of the key differentiating factors among the analyzed organizations is the geographic scope of their operations. While some companies focus exclusively on the domestic market, many are actively expanding abroad-both within the European Union and in non-European markets. Some firms are still focused on strengthening their local position, but almost all express international ambitions:

> "Currently, [we operate] on the Polish market, but of course we have plans for expansion." ~ Respondent 4.

Companies operating internationally are building business models based on export sales, international distribution, participation in overseas industry events, or establishing subsidiaries. Their market presence often spans dozens of countries.

> *"International. At the moment, we're present in about 12 markets, offering decap and disaster recovery solutions. In the West, we mainly provide source code protection solutions. Europe, the United States, and South America." ~ Respondent 6.*

Expansion directions most frequently include Central and Eastern Europe, the European Union, the United States, Southeast Asia, the Middle East, and selected African markets. For many companies, these are less saturated areas that are more receptive to new technologies and relatively open to innovative approaches.

> *"[…] These are developing markets or those in a growth phase. Markets not yet saturated with products, not locked down." ~ Respondent 13.*

Regulatory aspects are also an important factor. The unification of regulations within the EU (e.g., GDPR, NIS2) and the ubiquity of cyber threats make many companies view their products as naturally scalable.

[45] Raport "Polski rynek cyberbezpieczeństwa 2023–2028". Polski Klaster Cyberbezpieczeństwa #CyberMadeInPoland, Październik. 2023, s. 141-142.
[46] Artykuł w portalu branżowym „To będą nowe polskie akceleratory. PARP ogłasza wyniki Startup Booster Poland – Smart UP." MamStartup, 2024. [Access: 18.04.2025]
[47] Strona internetowa PFR "Dla działań wspierających rozwój technologii o potencjale podwójnego przeznaczenia". Polski Fundusz Rozwoju S.A., 2024. [Access: 18.04.2025]

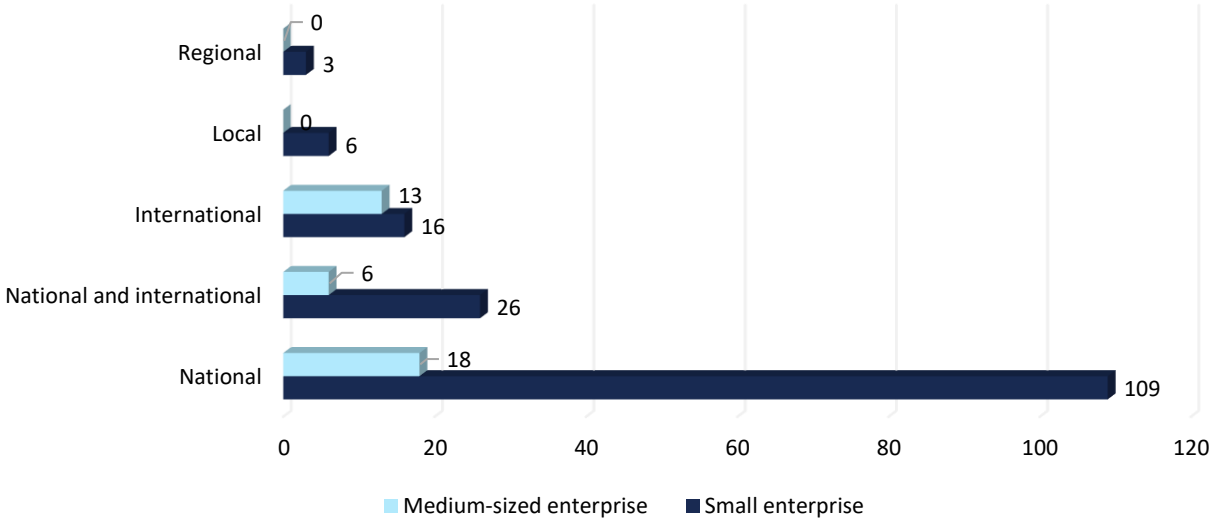
"The product is entirely written in English […], meaning it only supports the English language, so our expansion in Poland is really more of a warm-up for us." ~ Respondent 8.

Despite increasing international activity, many companies face real entry barriers to new markets. Challenges include complex procurement procedures, cultural and organizational differences, and high costs of sales and promotion.

"There are cultures focused on relationship-based business, where finding the right partner can quickly translate into revenue […]. And there are very transactional cultures, where that has little value and they take a binary, product-focused approach." ~ Respondent 13.

The following chart presents the distribution of business reach among the companies participating in the cybersecurity sector survey. While the majority of respondents operate primarily in the domestic market, a significant number also have an international presence.

Chart 31. What is the geographic scope of your company's operations? (N=197)



Source: IBC Advisory S.A. analyses based on CAWI survey.

The vast majority of small enterprises declared that their operations are domestic in scope - this response was selected by 109 companies. Among medium-sized enterprises, domestic reach also prevailed, indicated by 18 respondents.

Operations combining both domestic and international markets are carried out by 26 small and 6 medium-sized companies. Meanwhile, exclusively international operations were reported by 16 small and 13 medium-sized enterprises.

Local-level activity was indicated much less frequently (6 small firms), as was regional-level activity (3 small firms). None of the medium-sized enterprises reported operating at these levels.

These results show that while domestic operations remain the dominant model among respondents, a significant share of both small and medium-sized companies are also expanding into foreign markets.

An analysis of the responses reveals that companies in the cybersecurity sector most frequently operate in Western and Northern Europe, as well as in the United States. The internationalization strategy of Polish cybersecurity companies largely relies on establishing partnerships in foreign markets to support their development locally (through partner channels). In parallel with expansion, companies also engage in direct sales activities in selected foreign markets. Observing the business dynamics, the most common model is partner-channel sales for product companies and direct sales for service providers.

The most common expansion destinations include:

1. Germany and France, due to high demand for IT security services in these countries;
2. The United Kingdom and the Netherlands, home to numerous technology centers and startup hubs;

3. Switzerland and the Czech Republic, which are attractive in terms of both regulation and investment;
4. The United States, as a key global market for cybersecurity solutions;
5. The Baltic States (Lithuania, Latvia) and Sweden, which are gaining importance due to support from EU digitalization programs.

At the same time, the analysis of the #CyberMadeInPoland Cluster also indicates directions that were less prominent in the survey. The main countries targeted for international operations (ranked by frequency of indication from most to least interest) include[48]:

- United States (highest level of interest, although only a few firms have successfully carried out sales operations there);
- DACH countries, primarily Germany;
- Central and Eastern Europe (Romania, Czech Republic, Bulgaria, Hungary, Lithuania, Latvia);
- United Kingdom;
- Other Western European countries (Italy, Benelux, Spain, France);
- Nordic countries;
- The Balkans;
- Post-Soviet countries (Uzbekistan, Kazakhstan);
- United Arab Emirates (and other Gulf countries);
- Turkey;
- Asia (Philippines, Malaysia, Mongolia);
- Africa;
- South American countries.

To establish international business relationships, companies often participate in key trade fairs in target markets. They are also increasingly involved in support activities coordinated by Polish Trade Offices and Embassies.

Types of support most commonly used by Polish firms for international expansion include:

- **"Go to Brand" grant** by PARP - a program aimed at promoting Polish product brands from the SME sector on foreign markets. Funding could be used for purchasing booths at trade shows, business travel, participation in conferences and seminars, and marketing activities[49].
- **"Polish Technological Bridges" (Polskie Mosty Technologiczne)** - a program by the Polish Investment and Trade Agency (PAIH) that supports the promotion and internationalization of innovative companies. PAIH experts provide consulting and workshop-based support for developing a foreign market expansion strategy[50].
- **Participation in national stands** organized by PAIH.
- **Participation in regional stands** organized by individual Voivodeships.
- **Participation in trade missions** organized by local Foreign Trade Offices.

Due to limited publicly available data, it is difficult to determine how many analyzed companies are conducting international expansion and can be classified as operating globally. Since cyberspace has no borders, sales and implementation of cybersecurity solutions generally do not face significant technical or logistical barriers. However, international sales typically require compliance with local regulations. Within the EU, cybersecurity rules tend to be harmonized (e.g., the NIS2 Directive), but each member state may expand on the directive, requiring companies to familiarize themselves with and adapt to specific national provisions.

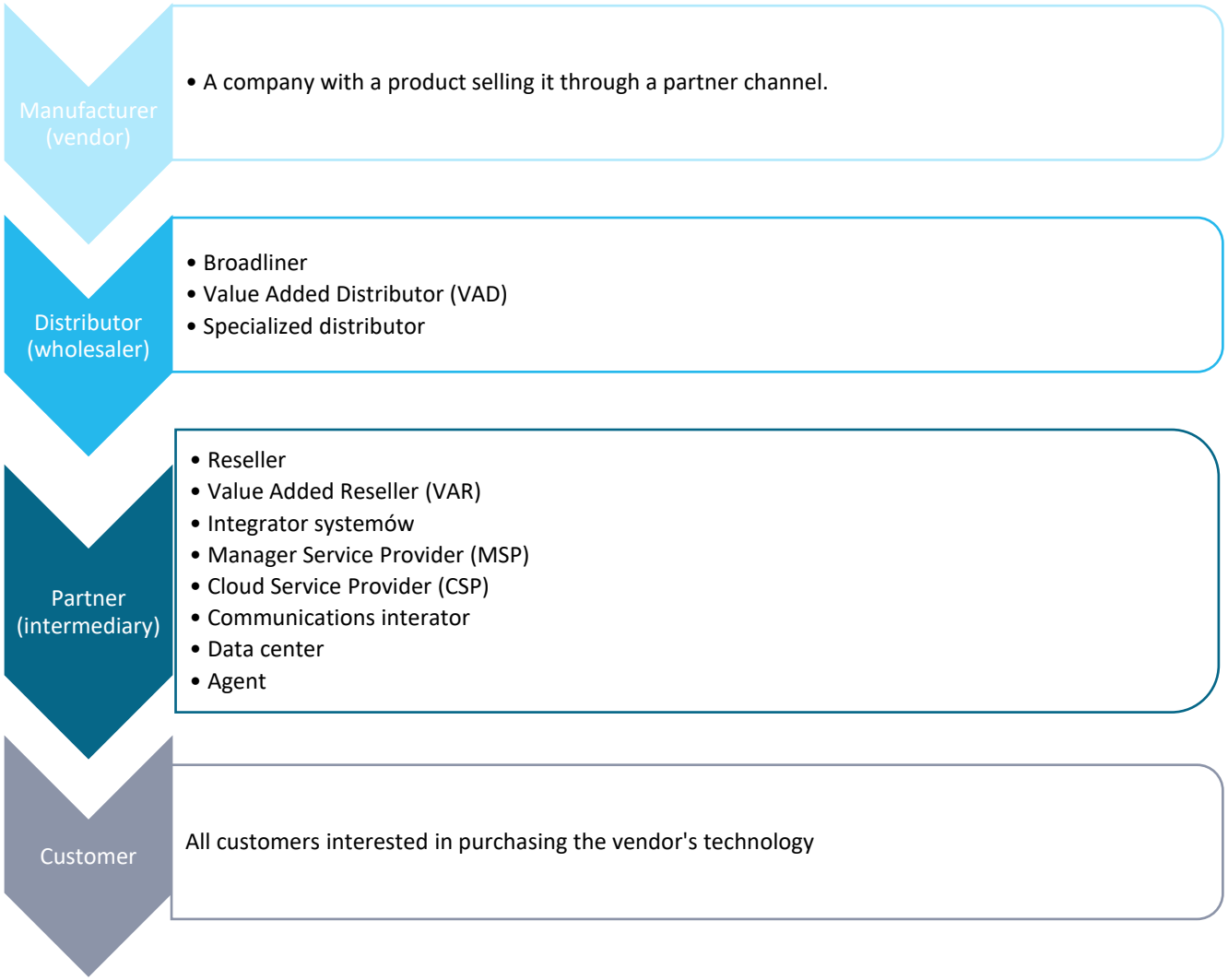
The biggest challenges to foreign sales include identifying suitable partners (integrators, distributors, or resellers) and adapting products or services to local legal conditions and languages (where required).

[48] Based on internal materials of the Cluster #CyberMadeInPoland.
[49] Strona internetowa PARP "Go to Brand." Polska Agencja Rozwoju Przedsiębiorczości (PARP). [Access: 18.04.2025]
[50] Strona internetowa PAIH "O projekcie – Polskie Mosty Technologiczne." Polska Agencja Inwestycji i Handlu (PAIH). [Access: 18.04.2025]

2.6. Analysis of Cooperative Links

Cooperation among companies on the Polish market is primarily driven by the creation of partner channels, product integration, and mutual service sales. Partnership cooperation typically follows standard models, where a vendor seeks out a distributor or partner who then promotes and sells the solution to a broader customer base.

Figure 1. Cooperative Links



Source: Based on data analyses by IBC Advisory S.A.

The integration of company products involves mutual adaptation of software with another product, resulting in complementary functionality for the client and expanding sales opportunities for both companies (as they can then recommend each other's solutions as complementary products). Furthermore, integrators carrying out large-scale projects benefit from a wider range of options for specific implementations.

Another common cooperative practice is the mutual resale of services. When a company lacks competencies in an area required by the client, it seeks an appropriate partner to fulfill that need. A good example is law firms that offer compliance services related to specific legal regulations. When they identify shortcomings or client needs, they can directly recommend a partner capable of delivering the required service.

Chapter 3

Barriers and development needs of Polish SMEs in the cybersecurity sector

3.1. Growth Barriers - Financial, Organizational, Regulatory

The cybersecurity sector in Poland is developing rapidly, with its directions shaped by technological advancements and a shifting geopolitical landscape. Based on the conducted qualitative and quantitative research, key trends and needs have been identified that will significantly influence the functioning and transformation of the industry in the coming years.

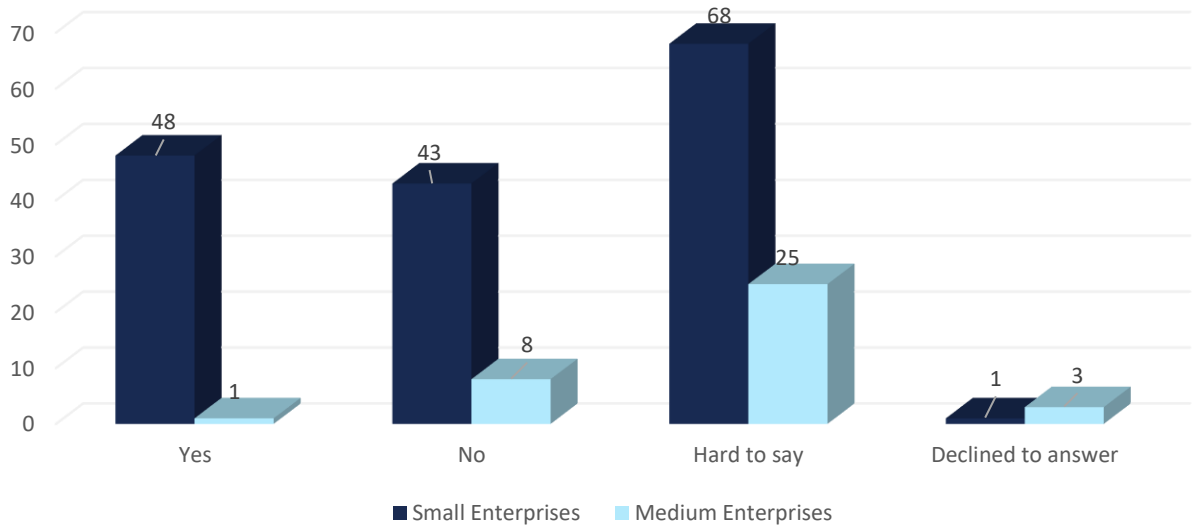
At the same time, the research revealed significant development barriers: low market awareness, difficulties in selling solutions that are unknown to the user, lack of systemic support for international expansion, and the dominance of global brands. Additional challenges include staff shortages, a lack of sales competencies, a low level of industry cooperation, and an unclear legal and tax environment.

To fully realize the potential of the Polish cybersecurity sector, systemic actions combining education, legislative support, promotion, and company professionalization are needed. Only coordinated efforts from all stakeholders can build a strong, resilient, and innovative digital security ecosystem.

The chart below presents the most frequently cited reasons for companies in the cybersecurity sector abandoning expansion plans. The analysis covers market and financial barriers, as well as organizational and strategic factors. The data includes both closed- and open-ended responses, offering insight into the diverse motivations and constraints that influence companies' development decisions.

The chart also illustrates to what extent companies in the cybersecurity sector identify development barriers that may hinder their further growth.

Chart 32. Does your company face any development barriers? (N=197)



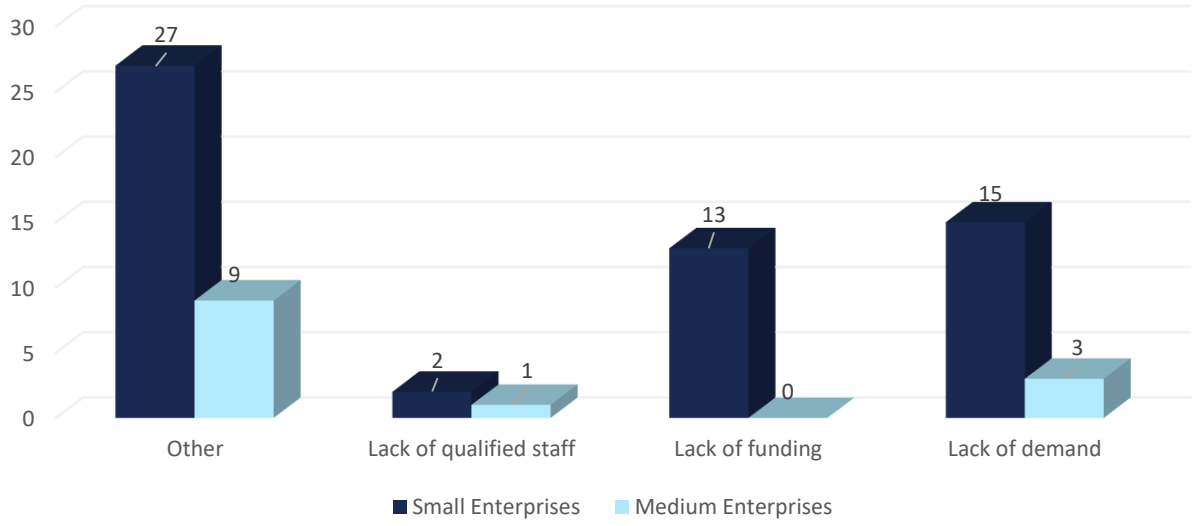
Source: IBC Advisory S.A. analyses based on CAWI survey.

Among respondents, the most common answer to the question about the existence of development barriers was "hard to say." This response was given by as many as 68 small and 25 medium-sized enterprises. The existence of development barriers was confirmed by 48 small companies, while only one medium-sized company reported facing such obstacles. A total of 51 companies-43 small and 8 medium-sized-declared no barriers. Only a few respondents refused to answer (1 small and 3 medium-sized enterprises). These figures may suggest that many companies lack a clear opinion on

development obstacles, which could stem from the absence of systematic barrier analysis or the difficulty in identifying them.

Companies that do not plan to expand their operations were asked to specify the main reason for this.

Chart 33. If you do not plan to expand your operations, what is the main reason? (N=70)



Source: IBC Advisory S.A. analyses based on CAWI survey.

A total of 18 companies declared that a lack of demand for their products or services is holding them back from expanding their operations. This indicates that a significant portion of enterprises perceives market limitations preventing effective growth-lack of demand may stem from market saturation, industry-specific constraints, or barriers to entering new segments.

Also 13 companies reported insufficient financing, highlighting real capital constraints and difficulties in obtaining funds necessary for development. Limited access to external financing (public or private) can effectively block investment activities, even when a company has the necessary potential and know-how.

For 3 companies, the barrier was the lack of qualified personnel, emphasizing the problem of talent shortages-particularly relevant in sectors requiring highly specialized skills, such as cybersecurity and advanced technologies.

An analysis of open responses provided under the "Other (please specify)" category revealed that many companies do not reject growth altogether but instead pursue alternative strategies or focus on consolidating and optimizing their current operations.

Several respondents pointed to a focus on their current business model, aiming to scale or refine it. Statements like “focus on the implemented business model,” “improving current services,” or “scaling the existing model” suggest that companies are engaged in development efforts but not necessarily in the form of geographical or operational expansion.

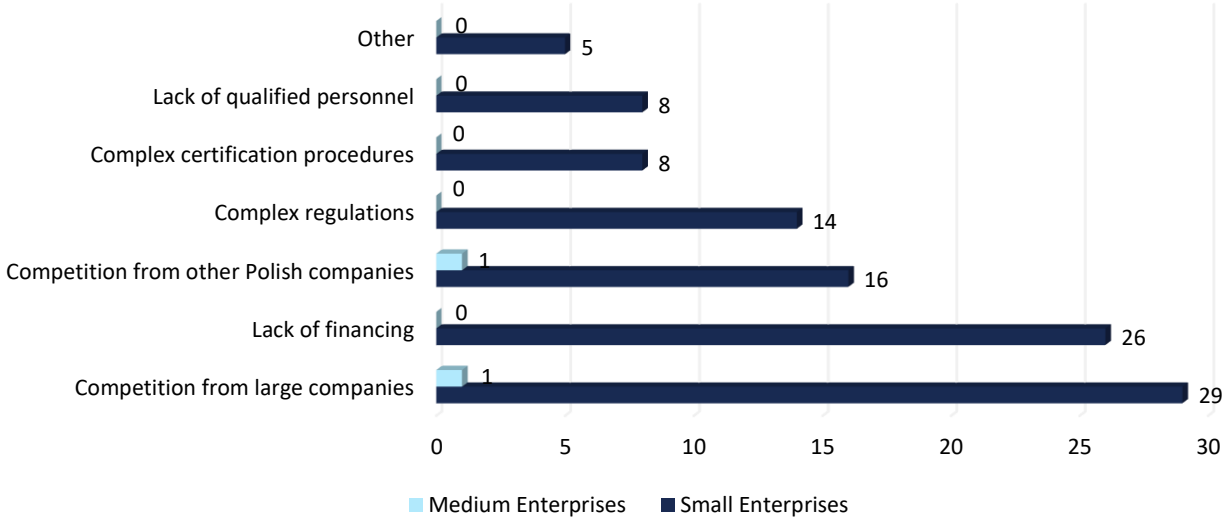
A recurring motivation was the desire to maintain the current size of the company, which is perceived as optimal-e.g., “the company’s current size is sufficient for us,” “we are developing within our current scope.” These responses reflect a conscious strategy of stabilization and risk management.

Other respondents mentioned prioritization of other types of investments, such as “other investment plans,” “additional income source,” or “reorganization,” indicating that financial and organizational resources are being directed toward modernization, restructuring, or diversification rather than expansion.

There were also individual responses pointing to external constraints, such as “lack of land for building telecom networks; network duplication is uneconomical,” highlighting that in some industries, growth may be restricted not by a lack of willingness, but by market or infrastructural limitations.

Chart below presents the most commonly cited barriers currently posing the greatest challenges to the growth of companies operating in the cybersecurity sector. Respondents identified both external constraints (such as competition or regulation) and internal ones (such as lack of funding, personnel, or skills).

Chart 34. What are the most significant development challenges currently facing your company? (N=49)



Source: IBC Advisory S.A. analyses based on CAWI survey.

Among the development barriers, the most frequently mentioned challenge was competition from large international companies-29 respondents identified this as an issue. SMEs in the cybersecurity sector struggle to compete with global players who have greater resources, stronger brand recognition, and operational scale.

The second most cited barrier was lack of financing, with 26 mentions. Companies often face difficulties securing capital for growth, innovation, or expansion, whether from public or private sources.

Competition from other Polish firms was indicated by 17 companies as a barrier, which may point to a saturated market, pricing pressure, or rivalry in niche segments.

Complex regulations were identified as a challenge by 15 respondents. Companies view the legal framework as opaque, unstable, or not aligned with market realities, which hinders planning and the implementation of development strategies.

Other frequently mentioned challenges included:

- Complicated certification procedures for products/services - 9 mentions;
- Lack of qualified personnel - 8 mentions;
- Other factors - also 8 mentions, including high operating costs (such as taxes and the “Polski Ład” reform), shortage of sales specialists, difficulties in securing R&D funding (due to required own contribution), and regulatory delays or inconsistencies. Additional concerns included low cybersecurity awareness among public institutions, underdevelopment of domestic infrastructure technologies, management teams’ competency gaps, and the high costs of effective solutions.

Low Market Awareness and the Challenge of Selling an "Invisible Product"

One of the most frequently cited issues by respondents was the persistently low market awareness-both among small and large enterprises-regarding the scale of digital threats and the real value of cybersecurity investments. For many clients, data and IT system protection is seen more as an unnecessary cost than a strategic business priority. This is especially true for organizations outside of regulated sectors, where certification or implementation of advanced security solutions does not generate direct profit and is thus deprioritized. As one respondent noted:

> *"[...] there's no real benefit to having a cybersecurity certification. So for us, I think the main blocker [...] is showing how cybersecurity can be a benefit-because the benefit of 'not being attacked' simply doesn't sell." ~ Respondent 14.*

This perception significantly impedes the commercialization of cybersecurity solutions and lowers organizations' willingness to invest in prevention and long-term protection.

In many corporations, cybersecurity departments lack their own budgets or decision-making autonomy. Expenditures are only approved when legally required:

> *"If a corporation in Poland-meaning an international company-even has a cybersecurity department, that department very rarely has its own budget." ~ Respondent 5.*

Such an approach not only limits demand for advanced solutions but also reinforces the notion that cybersecurity is a cost, not an investment.

Global competition further exacerbates challenges. U.S. and Asian companies, supported financially and politically by their governments, dominate not only global markets but increasingly the EU as well. Local suppliers have limited access to public tenders and budgets. One entrepreneur summarized the sector's concerns:

> *"At the end of the day, in some public institutions in Europe, security is partly ensured by solutions produced in India and sold by American entities. And I don't think that's ideal, even though it's not always the case. [...] For us to be as effective globally as large American companies, we simply need more clients and higher revenues to invest in scaling our global presence." ~ Respondent 10.*

Stagnation Trap and Innovation Barriers

The pace of technological change remains a major challenge. Cyber threats evolve rapidly, requiring continuous solution updates and investment in R&D. Smaller companies, lacking adequate resources, may fall behind, leading to marginalization:

> *"[...] a threat is the rapid pace of evolutionary change and of cyber threats themselves, because it demands constant investment in R&D. [...] Competition is also healthy for the market." ~ Respondent 11.*

Stagnation poses a serious threat to the industry's future. Unlike other sectors, cybersecurity does not tolerate standstill. As one company representative put it: "This is not an industry where you can stand still. If we don't grow, the competition will push us out soon". Without continuous product development and innovation, even previously successful companies can quickly lose their market position.

Lack of Systemic Support and Limited Expansion Opportunities

Another key limitation is the lack of institutional support for companies aiming to expand internationally. Unlike in countries like the U.S. or China, where cybersecurity exports are part of national policy (including funding, lobbying, regulatory support, and strategic market access), Polish firms are largely on their own. There is no cohesive export infrastructure, support for international certification, participation in foreign public projects, or strategic advisory services.

...] the main barrier is the ability to obtain financing for technology development. [...] Just look at the U.S. and its international expansion-this wouldn't be possible without governmental support and funding. The government's role is crucial." ~ Respondent 3.

Even tech-strong firms often fail to win large foreign contracts because purchasing decisions are made outside of Poland-at international headquarters.

Respondents point out that even when formally invited to international events, companies lack the financial tools to participate meaningfully:

"[...] PAIH invites us-yes, we're on their contact lists-but the invitations are sporadic and individual for specific events or trade fairs, and there's no funding attached. [...] For us, the real barrier is entry costs-travel, accommodation-so it would be great if funding became available." ~ Respondent 4.

In this context, even with competitive technology, Polish companies often lose to U.S. or Asian firms operating under more favorable financial and regulatory conditions. What they need are not occasional event invitations, but comprehensive support programs-economic missions, export training, and international marketing assistance. Without such actions, their ability to compete globally remains limited.

Dominance of Foreign Brands

The Polish market is dominated by large, recognizable companies-mainly from the U.S.-that have not only more capital and personnel but also international reputations reinforced by inclusion in industry reports. These firms enjoy a high level of trust, even in Poland, meaning that domestic providers are often overlooked despite having comparable or even superior competencies:

"[...] there's huge competition from U.S. companies, and we often don't get a chance to speak. [...] Where really big money is involved, we have a harder time-even in our own country. Abroad, we're seen as a global player. For example, in Rwanda, we're running a strategic defense project. But winning similar contracts in Poland would be extremely difficult." ~ Respondent 2.

A lack of media and marketing visibility is another issue. Polish companies rarely appear in industry rankings or comparisons, and as a result, are often not considered during purchasing decisions-even domestically.

Company Size and the Scale of Challenges - "Too Small to Play Globally"

One of the most visible and frequently cited barriers is the small scale of many cybersecurity companies operating in Poland. This especially affects young, innovative entities such as start-ups and specialized micro or small enterprises, which lack the financial, human, and organizational resources to compete on equal footing with large players-domestically or internationally.

These firms struggle to fund certifications, develop marketing infrastructure, attend industry trade shows and conferences, and conduct lobbying or international sales:

"Startups practically don't exist in Poland. [...] Why aren't there products? Because it's hard-besides all the boring PR and business stuff, you have to actually build the product. And product development is always prone to 50% error-if you plan for six months, it takes a year; if you budget half a million, it ends up costing a million." ~ Respondent 5.

"When it comes to product development, the bar is set very high, because cybersecurity involves the most expensive specialists on the market, so R&D projects-honestly, I wouldn't impose any limits here. There must certainly be openness. As for those grant programs for certification, I'd say a minimum of PLN 1.5-2 million per company is needed to do it professionally." ~ Respondent 4.

While large companies with capital and resources are able to adapt swiftly to regulatory changes (such as the NIS2 Directive or the CRA Regulation), smaller entities often fail to keep up with the pace of legislative change, which puts them at risk of being excluded from supply chains. In practice, this leads to the marginalization of innovative but underfunded solutions.

Location: Poland as a Decision-Making Periphery

Another significant development barrier is geographic location-not only in terms of physical presence, but above all regarding the decision-making structure that dominates the European technology market. Although Polish companies operate within the common EU market, they often point out that real purchasing, procurement, and investment decisions are made in foreign corporate headquarters-mainly in Western Europe.

This power imbalance means that local branches of clients operating in Poland lack decision-making authority, and entering global procurement structures requires tremendous effort, connections, presence, and financial resources.

> *"[…] We can't just approach the local branch of a bank in Poland, because a branch is just a branch, but its HQ is in France, Portugal, or Norway. We have very few companies here with local decision centers. That's why the state should support us in international expansion, because on our own we have very limited possibilities […]" ~ Respondent 8.*

The situation is worsened by the fact that many tenders conducted locally in Poland are structured in a way that excludes smaller entities. The criteria are often disproportionately strict-as if designed for enterprise-level suppliers-which makes it very difficult for SMEs to participate meaningfully in the public procurement market.

> *"There's a tender for a system of our class, and we're basically excluded because the requirements read like someone's building a spaceship and has been to Mars three times and now wants a spacecraft of similar caliber. […] In our domestic market, we have to prove we're not a camel, even though we have strong references outside of Poland […]" ~ Respondent 2.*

Staff Shortages and Lack of Experts

The cybersecurity sector is increasingly affected by a shortage of qualified specialists. Despite Poland having a strong IT sector, the narrow field of cybersecurity lacks professionals with a high level of technical training and strategic capabilities. This issue concerns not only recruitment, but also knowledge and competence management within organizations.

> *"[…] The barrier will be hiring specialists, because we'll eventually run out, and we'll have to introduce solid internal education to calibrate knowledge within the organization […]" ~ Respondent 6.*

The solution lies in developing dedicated educational pathways, certification programs, and closer collaboration between universities and industry-helping align market expectations with graduates' actual skills.

Innovation is also held back by a lack of real connection between academia and business. Although companies are open to collaboration, there are no mechanisms enabling cooperation with universities or research centers. One industry expert put it directly:

> *"[…] We definitely need to invest more in linking business with academia. We do a lot of work with scientists and have various experiences, but there really isn't a platform to connect these two worlds-specifically in cybersecurity. That would be very valuable." ~Respondent 4.*

Without systemic cooperation programs, technology accelerators, and incentives for researchers, knowledge remains trapped within academia and doesn't translate into real-world products.

The sector also struggles with a competence gap. The number of available experts doesn't meet the growing demand, and universities can't keep up with technology changes. Entrepreneurs are increasingly giving up on finding ready candidates and instead train employees from other sectors. As one interviewee put it:

"[…] When I hire people, I don't necessarily go for cybersecurity graduates, though I still think such schools should exist. I hire people from sectors like finance or energy and prefer to train them in cybersecurity myself […]" ~Respondent 8.

There is also a lack of public reskilling programs that could help bridge this talent gap.

Specialization - Technological Advantage or a Development Trap?

Many Polish cybersecurity companies stand out for their high level of technological specialization. They develop unique, often breakthrough solutions in the field of IT security. However, their focus on products rather than services or outsourcing often leads to scalability challenges.
They lack not only financial resources for promotion and expansion, but also sales capabilities, business experience, and access to proper distribution channels. As a result, despite technological advantages, these companies face difficulties in monetizing their innovations.

"[…] the problem with small enterprises is that while they have potential, they lack the means to spread their wings. It always comes down to capital-without it, nothing moves forward. And without money, you can't hire specialists." ~ Respondent 12.

Another problem lies in the mismatch between public funding programs and the technological realities of these firms. Public support is often generic, without accounting for technical nuances, the specific costs of certification, or the iterative nature of research and testing in cybersecurity.

Lack of Market Equality and the "Glass Ceiling" of Growth

Despite their innovation and high-quality solutions, Polish tech firms often face structural inequality in accessing public procurement and support programs. Even though their products are present in hundreds of locations worldwide, they do not have the same opportunities to carry out projects domestically.

"[…] Providing support or a competitive edge for Polish firms in public procurement is probably saying too much-you simply can't do that. But I wonder whether the European Union, as a whole, should reward European companies more. Not just American firms with EU branches, but genuinely European ones. […] In the U.S., local companies are always better positioned. […] They're seen more favorably. […] I'd rather see that support at the European level, in terms of competitiveness, rather than at the Polish national level." ~ Respondent 9.

Moreover, the absence of preferential treatment for domestic firms in public tenders contrasts with practices in countries such as the United States or Israel, where government institutions actively support national technology producers.

Organizational and Communication Barriers

Many companies-especially smaller ones founded by engineers and technical experts-struggle with commercializing their solutions. A key challenge is the inability to "tell the story" of their product in business terms that resonate with IT and budget decision-makers.

"[…] These companies grew to 3, 6, maybe 10 million over 6-10 years and then plateaued. Why? Most often because they were founded by cybersecurity specialists who know as much about business as I know about tanks-which is nothing. They brought in some clients, got traction through recommendations, but eventually lost sight of why they started the company in the first place." ~ Respondent 5.

There is a lack of sales, marketing, and strategic competencies that would enable scaling operations and reaching customers across various industries. What's needed is a professionalization of market communication, as well as support in managing the sales cycle and developing business partnerships.

Low Level of Collaboration and Absence of Industry Lobbying

The Polish cybersecurity sector is also characterized by a low level of internal cooperation. There is a lack of joint initiatives, advocacy efforts, and cohesive representation of sector interests to government institutions and at the international level. Companies operate in isolation, focusing on current leads rather than building lasting collaborative structures, consortia, or development funds.

This industry immaturity results in limited influence on regulatory policy, which in turn leads to legislative chaos, market voices being ignored in lawmaking, and missed opportunities for systemic preferences in national and EU public procurement.

Financial Gaps

One of the most frequently cited problems is the lack of growth capital-especially for startups and young tech firms. Entrepreneurs point out that the Polish venture capital market is still in its early stages, and R&D funding remains out of reach for many innovative but small companies.

"[…] In Poland, investment levels for tech startups are still very low compared to, say, the U.S."
~ Respondent 4.

This situation prevents companies from completing product development, conducting expensive certification, or taking the risk of entering new markets. As a result, many Polish companies-despite being technologically ready-are unable to move beyond a niche position.

Additionally, entrepreneurs emphasize the absence of effective bridge mechanisms to support companies beyond the MVP stage but before they reach profitability. There are recurring calls for the creation of development funds targeted at sensitive and high-value strategic technologies.

Bureaucratic, Legal, and Tax Barriers

It is also important to highlight the problematic legal and economic environment, which presents a significant burden for many companies. Onerous bureaucracy, frequent regulatory changes, non-transparent IT security rules, and high tax costs-especially burdensome for small and medium-sized enterprises-are all factors that effectively discourage investment and expansion.

Companies also report confusion around the EU legislation (e.g., GDPR, NIS2, CRA), which are often interpreted inconsistently, leading to legal uncertainty and inefficient allocation of resources to unnecessary or poorly defined requirements.

One of the most serious threats mentioned in interviews with sector representatives is overregulation. While the need to raise cybersecurity standards is evident, the way regulations are implemented often leads to excessive burdens, particularly for smaller entities. Especially problematic are the certification costs required by public-sector institutions and European bodies. As one respondent stated:

"[...] the Polish public administration can purchase any cybersecurity-related product provided it has certification such as EL4 or Common Criteria. [...] this overregulation at various levels is, in my opinion, a significant threat [...] We're talking about the SME sector here, and lobbying by international players may lead to the creation of unhelpful regulations." ~ Respondent 9.

Concerns are also raised that new regulations are driven not by genuine security concerns but rather by strong lobbying from foreign corporations aiming to eliminate local competition.

In public procurement, Polish companies still face systemic barriers that hinder their effective participation in tenders. Large foreign corporations often win, as tender documentation is crafted to suit their specifications.

"[…] it's harder in our own country […] Abroad, we are seen as an international company-just in Rwanda, for example, we're carrying out a very strategic defense project. In Poland […] I think it would be extremely difficult." ~ Respondent 2.

A thorough revision of procurement rules is needed-one that would favor local innovation, code security, certification process transparency, and compliance with EU regulations.

"[…] The Ministry identified the existence of Polish solution providers, wanted to learn more about them, and created some kind of procurement space […]" ~ Respondent 13.

Investment Challenges: Regulations, Bureaucracy, Uncertainty

Despite a clear willingness to invest and grow, company representatives point to serious barriers that slow down or complicate the implementation of their plans. Foremost are issues related to regulatory overload and the bureaucratic nature of public support systems-especially in the context of grant applications.

"Overregulation is definitely a threat to this industry-unnecessary regulations" ~ Respondent 9.

Firms also point to the significant burden posed by the new EU legislation. Examples include the requirements of DORA, eIDAS and NIS2 directive, which necessitate renegotiating contracts, engaging legal teams, and adapting documentation for hundreds of clients-resulting in delays in product development:

"[…] new regulations are currently a huge challenge. One issue is the need to sign amendments with all existing clients, which took an enormous amount of time from our legal department to process and execute" ~ Respondent 15.

In addition, respondents stress the unpredictability of the legal environment and the lack of clear interpretations of regulations, which leads to investment caution and the postponement of some projects.

Risk Management Mentality: "It'll Work Out Somehow"

Finally, a cultural and mental barrier should also be noted-related to risk management, strategic planning, and investment in security. Many companies in Poland still operate with a survival-oriented mindset focused on short-term operations rather than long-term growth.

"We are a society that was taught to cope during years of poverty, that everything was done [...] with metaphorical rubber bands, that somehow we'll manage, somehow it will hold together. So that's a trait that persists." ~ Respondent 7.

Additionally, low awareness of threats among SMEs hampers the ability to market cybersecurity as a tangible, measurable value. In many cases, data protection is seen more as a costly luxury than a business necessity.

The Polish cybersecurity sector is growing dynamically, but its growth is slowed by numerous systemic, market, and organizational barriers. One of the main challenges is the lack of widespread access to both public and private funding. Despite the existence of various support programs, most companies do not take advantage of them due to complex procedures, lack of information, or insufficient organizational resources.

Another issue is the low market awareness of actual threats and the value of cybersecurity. Many clients do not view cybersecurity investment as a strategic priority but rather as an unnecessary cost-especially outside regulated sectors, where the lack of legal obligations results in a low willingness to implement security solutions. Cybersecurity departments in large organizations often lack their own budgets, which significantly hinders market development.

Many respondents also pointed to strong competition from global players, especially American and Asian firms. These entities have greater resources, better market access, and state support. Poland lacks a coherent policy for supporting the export of cybersecurity solutions. Companies indicate a shortage of economic missions, effective certification support, and promotion in foreign markets. Even invitations to trade fairs and events are often not linked to funding for participation.

A major barrier also remains the scale of operations. Most Polish cybersecurity firms are SMEs that lack the resources to compete globally. Smaller companies cannot afford the costs of certification, PR, or presence in industry reports. Public procurement is dominated by requirements tailored to large corporations, which effectively excludes local providers. Even if Polish companies are carrying out strategic projects abroad, at home they face formal barriers and a lack of trust.

Another critical issue is the shortage of specialists. The sector is struggling with a talent deficit, especially in areas requiring advanced technical and strategic competencies. Universities are not keeping pace with training, and reskilling programs are insufficient. Entrepreneurs are increasingly investing in internal development and retraining of employees from other industries. At the same time, there is a lack of cooperation platforms between science and business, which hampers the commercialization of innovation.

A further development barrier is the lack of sales and strategic competencies in many technology firms. Companies founded by engineers often struggle to scale, lacking the ability to create coherent business models and sales narratives. There is a need for professional market communication, mentoring support, and education in growth management.

Equally serious is the lack of internal cooperation within the sector. Companies rarely form consortia, conduct joint advocacy efforts, or engage in shaping regulatory policy. The industry lacks representation that could effectively communicate its needs to government bodies. Low levels of collaboration lead to dispersed resources and weaken the sector's position in public discourse.

The regulatory environment is also problematic. The implementation of EU legislation is often chaotic, and certification requirements are costly and mismatched to SMEs' capabilities. Companies point to overregulation and lobbying by large corporations that influence the regulatory landscape to eliminate competition. Lack of equal opportunity in public procurement and the exclusion of local suppliers remain major systemic barriers.

Finally, it is important to note that many of the described issues also stem from a cultural approach to risk. Polish companies often act reactively, focusing on day-to-day operations rather than long-term development. Strategic thinking about cybersecurity as an investment and competitive advantage is lacking. The "it'll work out somehow" mentality and low levels of planning hinder the creation of scalable and resilient business models.

To fully unlock the potential of Poland's cybersecurity sector, coordinated systemic actions are necessary. Financial support systems must be reformed, regulations simplified, cooperation mechanisms between academia and business established, and professional management and sales structures supported. Without such measures, many innovative Polish companies will remain on the periphery of the global market-despite their technological edge.

The cybersecurity sector in Poland is developing dynamically, shaped by both emerging technologies and geopolitical factors. Based on the conducted qualitative and quantitative research, the most important trends and needs that will influence the industry in the coming years have been identified.

One of the key challenges is the prediction phase-anticipating potential threats. Although detection and response technologies are becoming increasingly effective, many organizations still lack tools for scenario-based risk analysis. This highlights the growing importance of threat intelligence and predictive analytics, which can shift the focus from reaction to prevention.

The public sector can play the role of an innovation catalyst by becoming a key client and a testing ground for domestic solutions. However, this requires investments in both technical and strategic competencies that will enable the effective use of the sector's potential.

Respondents in the qualitative research also emphasized the importance of diversity-especially regarding women's participation and the creation of inclusive teams. Cultural and competency diversity is seen as a driver of innovation and sectoral resilience in the face of future challenges.

At the same time, the study revealed several critical development barriers: low market awareness, difficulty in selling solutions that are invisible to users, lack of systemic support for foreign expansion, and the dominance of global brands.

Additional challenges include talent shortages, a lack of sales competencies, limited industry collaboration, and an opaque legal and tax environment.

To fully realize the potential of the Polish cybersecurity sector, systemic action is needed-combining education, legislative support, promotion, and the professionalization of companies. Only through the integrated efforts of all stakeholders can a strong, resilient, and innovative digital security ecosystem be built.

In a 2023 study conducted by the Polish Cybersecurity Cluster #CyberMadeInPoland, over 60% of respondents identified excessive solution cost as one of the key barriers to the development of the Polish cybersecurity market. Other major barriers included: lack of trust in lesser-known solutions (47.5%), lack of cybersecurity competencies within organizations (47.5%), low awareness among end users (45.5%), lack of knowledge about existing solutions (40.6%), too many regulations (38.6%), and insufficient number of cybersecurity professionals (17.8%)[51]. Furthermore, during a panel discussion organized by NCC-PL at the CYBERSEC Forum/EXPO 2023 in Katowice, speakers identified the most significant market entry barriers for small and medium-sized enterprises (SMEs) operating in the cybersecurity field in Poland-barriers that closely matched those outlined in the report. These included: Strong competition, Relatively small promotional budgets of domestic SMEs compared to larger market players, The perception of Polish products as lower quality and lack of client trust in domestic solutions, Limited access to cybersecurity specialists due to high employment costs, Challenges in utilizing EU funds to support SMEs, Low client awareness of cybersecurity threats and the need for protective solutions[52]. Other barriers mentioned included difficulties in obtaining client references and a lack of knowledge on how to improve competitiveness (as discussed during the VI Cybersecurity Forum in Karpacz)[53].

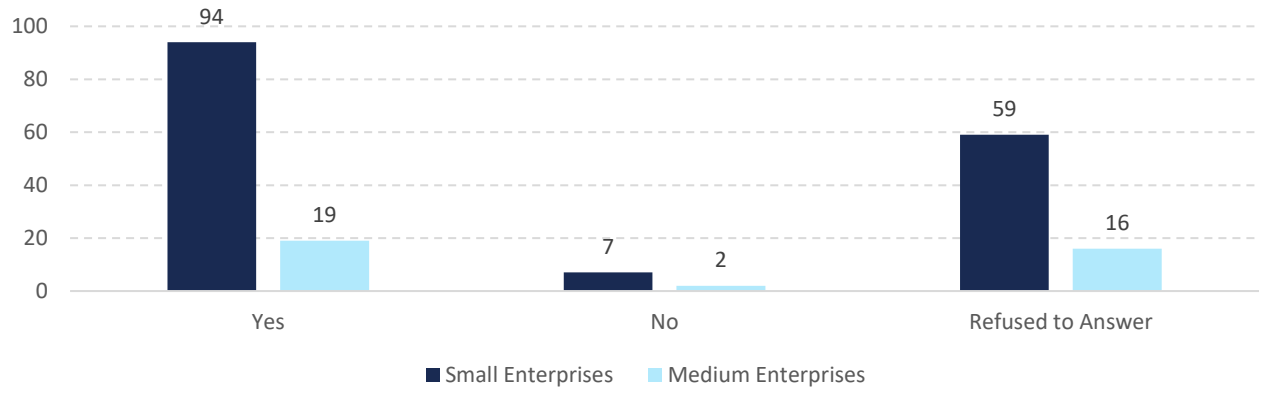
Although all companies operating in the cybersecurity sector face similar challenges, their nature varies depending on the size of the organization. Small firms struggle to attract clients, build credibility, and secure financing, while larger entities deal with regulatory pressure, IT infrastructure complexity, and operational costs. In both cases, key factors for success include investment in technology development, human resources, and appropriate sales and marketing strategies.

3.2. Regulations of the Polish Cybersecurity Market

The Impact of Regulations on the Operations of Cybersecurity Firms

The chart below illustrates the level of awareness among representatives of cybersecurity companies regarding two key EU pieces of cyber legislation - the Cyber Resilience Act (CRA) and the NIS2 Directive (on the security of network and information systems).

Chart 35. Are you familiar with the CRA and NIS2 regulations? (N=197)



Source: IBC Advisory S.A. analyses based on CAWI survey.

[51] Raport "Polski rynek cyberbezpieczeństwa 2023–2028". Polski Klaster Cyberbezpieczeństwa #CyberMadeInPoland, Październik. 2023, s. 125-126.
[52] Opis panelu „Szanse i Bariery dla MŚP działających w obszarze cyberbezpieczeństwa w Polsce" podczas Cybersec Forum w Katowicach, 2023 r. Gov.pl. [Access: 18.04.2025]
[53] Panel "Jak uczynić polskie cyber MŚP bardziej konkurencyjnymi", podczas VI Forum Cyberbezpieczeństwa w Karpaczu, 2024.

Respondents in the study were asked about their familiarity with the **Cyber Resilience Act (CRA)** and the **NIS2 Directive** (on the security of network and information systems). The majority of companies declared familiarity with this EU legislation - 94 small and 19 medium-sized enterprises responded "yes."

Only 7 small and 2 medium companies reported a lack of awareness, which may indicate increasing awareness of upcoming legal requirements among cybersecurity companies.
However, it is worth noting the relatively high number of non-responses - 59 small and 16 medium-sized companies did not declare their level of knowledge. This may suggest uncertainty about the question or a lack of clear understanding of NIS2 or CRA.

The vast majority of companies in in-depth interviews indicated familiarity with both NIS2 and CRA, although the NIS2 Directive is significantly better understood and, in many cases, already being implemented. CRA, as a more recent regulation, is often seen as a challenge for the coming months - companies are aware of the requirements, but not all have started the implementation process.

The impact of the regulations is considered significant, though not unequivocal. Some companies see the regulations as a positive development driver - forcing them to streamline processes, invest in cybersecurity, and raise awareness among clients and partners.

"In connection with NIS2, we're seeing increased interest in our products. […] There's a bit more movement in the market and interest in our devices because everything revolves around data security." ~ Respondent 1.

On the other hand, increasing administrative burdens, documentation requirements, and interpretive ambiguities are seen as serious development obstacles.

"[…] as for the new regulations, it's a huge effort right now. […] We do an enormous amount of work just to respond to inquiries because institutions are obliged to obtain such information, but no one really knows how to interpret it." ~ Respondent 15.

There is also a recurring theme regarding the need to adapt products and develop new functionalities in line with the directives, as well as expanding legal, audit, and compliance teams.

"[…] we definitely fall under CRA, and of course, this is going to be a more advanced CE marking, so we have to keep an eye on those requirements. We're not ready yet, but we're aware, and that's already half the battle. Then there's the NIS2 Directive, which we'll probably be subject to as well, although it's still unclear. […] We've implemented ISO 27001 and are certified, and we've also implemented 22301 (business continuity), though we're not certified in that one yet." ~ Respondent 4.

At the same time, regulations are also seen as a market opportunity, especially given the growing needs of SMEs who are only now beginning to invest in cybersecurity.

"Regulations are always a positive environment because the very act of issuing them makes even entities not directly affected realize that these things are important." ~ Respondent 9.

In summary, the NIS2 and CRA are perceived as necessary and inevitable, yet burdensome and time-consuming. Their impact on business operations is substantial - representing both challenges and market opportunities.

DORA - Financial Standards Impacting the Entire Industry

The DORA regulation is felt most in the context of increasing requirements from financial institutions. Companies report that new rules on digital security and operational resilience are becoming the de facto market standard - even when not formally applied to them. Polish cybersecurity SMEs, as subcontractors to institutions subject to DORA, must align their operations with the requirements imposed by their clients – particularly in areas such as business continuity, incident management, and compliance with information security policies.

"[…] DORA is essentially a norm in this area. Unfortunately, things aren't easy for us […] there's huge competition from American companies, and we often don't get a chance to be heard." ~ Respondent 2.

The strongest effect of DORA is visible in customer interest - especially from banks and insurers - in solutions related to business continuity, disaster recovery, and supply chain security.

"[…] DORA is aimed directly at financial institutions, and therefore these institutions - just like those fulfilling or wanting to fulfill NIS2 - aim to protect their data." ~ Respondent 6.

This regulation is seen as an evolution rather than a revolution - especially by companies already working with the financial sector and familiar with KNF (Polish Financial Supervision Authority) requirements. The change lies primarily in formalizing and structuring expectations toward technology providers..

"[…] The financial sector may not have cybersecurity completely down, but we could say they almost do." ~ Respondent 9.

At the same time, competitiveness is a concern - smaller European firms struggle to break through in tenders against large U.S. players with greater resources and market power.

"[…] Unfortunately, we don't have it easy, to put it bluntly, because there's huge competition from American companies, and we often don't get a voice." ~ Respondent 2.

DORA raises the bar significantly regarding security and operational resilience - not only for the financial sector but also for its technology vendors. In practice, it becomes a universal market standard - determining the ability to work with financial institutions and increasing pressure to professionalize processes. For cybersecurity firms, this means both new organizational challenges and the opportunity to build competitive advantage by aligning their offerings with the expectations of high-demand clients.
However, without support for smaller entities - particularly in interpreting regulations and accessing resources for adaptation - there is a risk of deepening market inequality.

Among cybersecurity companies, there is a relatively high level of awareness of EU legislation - 58% of respondents declare familiarity with the CRA and NIS2 acts. However, as many as 38% did not provide a clear answer, which may suggest uncertainty or a lack of decisiveness among respondents.

In in-depth interviews, companies more frequently and clearly understand the requirements of the NIS2 Directive, which is already being implemented in some cases. The CRA, on the other hand, is perceived as a new, complex challenge that is only beginning to be analyzed in terms of implementation.

Companies point out that while demanding, regulations may serve as a driver of development. They are often compared to GDPR - forcing process standardization, increasing demand for services, and raising customer awareness. Regulations also encourage investment in compliance, the expansion of legal teams, and the adaptation of products to formal requirements.

At the same time, criticism is voiced: companies are concerned about the rising cost of implementation, unclear legal interpretations, and the heavy documentation burden. CRA preparation is particularly problematic, as its requirements (e.g., CE marking) necessitate major changes in processes and product offerings.

Although formally directed at financial institutions, the DORA regulation has a clear impact on the entire technology provider ecosystem. Companies observe that DORA is becoming a *de facto* market standard that determines cooperation with banks and insurers. This reinforces the pressure to ensure operational resilience, disaster recovery, and supply chain security.

DORA is viewed as an evolution of the financial sector's existing requirements, but with stronger formal power. For companies, this means the need to further professionalize operations and expand security systems - often with limited resources.

Many interviewees emphasize that although the regulations create market opportunities, they favor large international players - especially from the United States. Smaller firms struggle to compete, which risks further deepening competitive inequality.

The cybersecurity sector expects government support in the areas of education, legal interpretation, and access to funding for the implementation of new requirements. There is also a need for certification instruments tailored to the realities of SMEs, not just large enterprises.

Ultimately, companies agree that NIS2, CRA, and DORA are inevitable and important, but at the same time require significant organizational, financial, and skill-based efforts. Their effective implementation requires cooperation between the private sector and public administration, as well as the introduction of support tools suited to companies of varying sizes.

Cybersecurity is one of the key challenges for the functioning of the modern digital economy. In the face of dynamically evolving cyber threats, EU countries, including Poland, are implementing comprehensive legal regulations that define the frameworks for data protection, cybersecurity, and digital resilience for institutions and enterprises. For small and medium-sized enterprises (cyber SMEs) operating in the cybersecurity market, new legal requirements mean the need to adapt operations - both as producers/distributors of solutions and as participants in the digital ecosystem.

Key Polish Regulations Shaping the Cybersecurity Market

The Act on the National Cybersecurity System (KSC)

This act imposes obligations on essential entities, including digital service providers, meaning that cyber SMEs that develop software or provide IT services must ensure compliance with requirements regarding risk management, incident detection and reporting, and appropriate protection measures. A revision of the KSC is currently underway to align it with the EU NIS2 directive, including expanding the scope of covered entities, tightening cyber resilience requirements, and increasing penalties for violations[54].

General Data Protection Regulation (GDPR)

For cyber SMEs as producers of IT solutions processing personal data, GDPR requires the design and implementation of security in accordance with the "privacy by design" principle. As part of the IT supply chain, SMEs are required to ensure compliance with data protection standards and support clients in fulfilling information obligations and responding to data breaches[55].

Poland's Cybersecurity Strategy

Poland also has a Cybersecurity Strategy - a document that sets out the state's long-term strategic goals in cybersecurity policy, identifies responsible entities, and outlines resources required for implementation.
The main goal of the Strategy is to enhance resilience to cyber threats and improve information protection in the public, military, and private sectors[56].

It also specifies actions related to strengthening IT infrastructure resilience, international cooperation, public awareness, and innovation in the cybersecurity sector. The current strategy (2019-2024) remains in force until the release of a new one for 2025-2029, which is currently undergoing inter-ministerial consultations[57].

Key EU Regulations Shaping the Polish Cybersecurity Market

Cybersecurity Act

This regulation is particularly important for cyber SMEs that manufacture hardware and software. The obligation to meet the requirements of European certification schemes (with one of three assurance levels: basic, substantial, or high) means

[54] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Dz.U. 2018, poz. 1560.
[55] Artykuł "Na czym polega ochrona danych osobowych RODO? Rozporządzenie RODO w pigułce". EY, 2025. [Access: 15.04.2025]
[56] Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024. Ministerstwo Cyfryzacji, 2019. [Access: 18.04.2025]
[57] Ibidem.

investing in security testing, technical documentation, and compliance with certification procedures. Obtaining a certificate, however, may become a competitive advantage and enable access to public or international markets[58].

DORA (Digital Operational Resilience Act)

Although directly aimed at the financial sector, DORA also affects cyber SMEs as ICT providers. Companies supplying services or products to financial institutions must demonstrate compliance with their ICT risk management strategies, including incident monitoring procedures, business continuity plans, and information security policies. For many SMEs, this means building internal capabilities in compliance and cyber risk management[59].

NIS2 Directive

The NIS2 Directive expands cybersecurity regulation to cover more sectors and companies, including some SMEs. SMEs may be directly covered by NIS2 if they provide services in a regulated sector and are deemed essential or important entities, or indirectly as suppliers or clients of such entities. This introduces new cybersecurity obligations, including risk management, supply chain security, employee training, and incident reporting[60].

CER Directive (Critical Entities Resilience)

The CER Directive, while not directly affecting most SMEs, may still have an indirect impact. It focuses on increasing the resilience of entities that provide essential services for the economy and society (critical entities). If SMEs are suppliers or subcontractors to such entities, they may be required to meet certain cybersecurity standards to ensure service continuity and process security[61]. Together with NIS2, the CER directive forms a complementary and harmonized legal framework for ensuring the continuity and resilience (both physical and digital) of essential services.

Cyber Resilience Act (CRA)

The implementation of the CRA aims to improve user safety and reduce key vulnerabilities in software and electronic devices. The new rules require manufacturers to incorporate cybersecurity principles at the design stage of products and services and to ensure protection throughout their entire lifecycle. Manufacturers will also be required to manage vulnerabilities effectively, ensuring that all security flaws are identified and patched for a defined period after the product is launched.[62].

Opportunities for SMEs in the Cybersecurity Sector

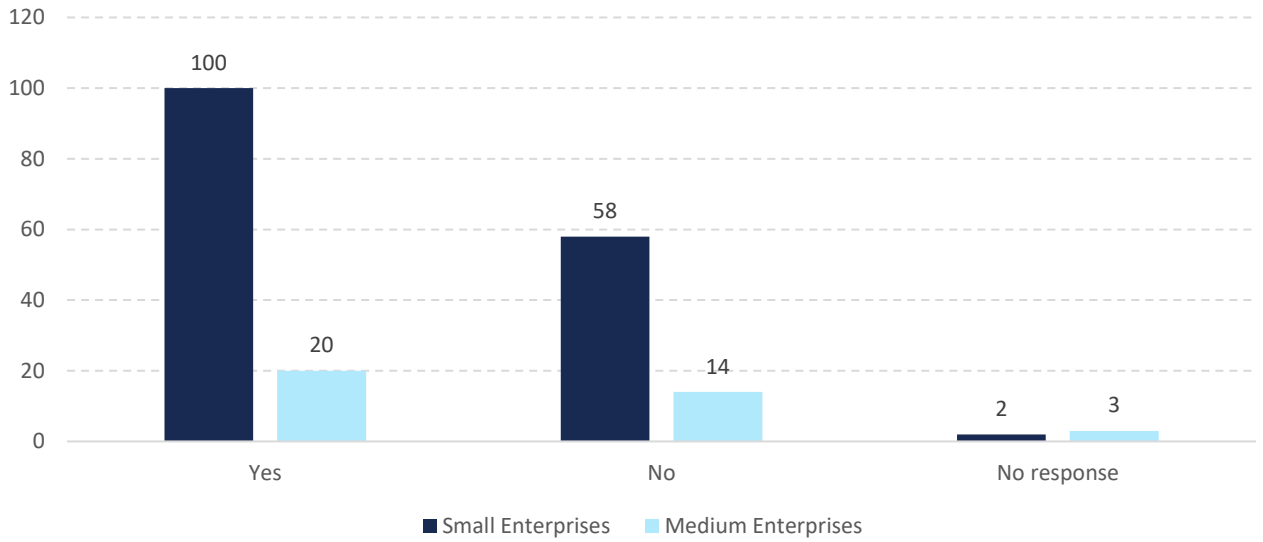
Despite increasing regulatory obligations, the new legislation creates significant growth opportunities for SMEs. This will undoubtedly include rising demand for auditing services, penetration testing, and compliance consulting, as well as the possibility of certifying products in accordance with EU requirements - a factor that facilitates expansion into foreign markets. SMEs may also benefit from collaboration with the public sector and entities covered by the highlighted legal acts.

[58] Rozporządzenie (UE) 2019/881 w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych. Dz.U. L 151 z 07.06.2019, s. 15-69.
[59] Rozporządzenie (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego oraz zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014 i (UE) 2019/2033. Dz.U. L 333 z 27.12.2022. s. 1-65.
[60] Dyrektywa (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (NIS2). Dz.U. L 333 z 27.12.2022, s. 80– 152.
[61] Dyrektywa (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE. Dz.U. L 333 z 27.12.2022, s. 164–196.
[62] Rozporządzenie (UE) 2024/2847 z dnia 12 marca 2024 r. w sprawie horyzontalnych wymagań dotyczących cyberbezpieczeństwa dla produktów z elementami cyfrowymi oraz zmieniające rozporządzenie (UE) 2019/1020. Dz.U. L 333 z 27.12.2024, s. 1–65.

3.3. Expectations Toward the Institutional and Legislative Environment

The study also included an analysis of whether the surveyed companies believed they could overcome development barriers independently.

Chart 36. In your opinion, can development barriers be overcome at the enterprise level? (N=197)

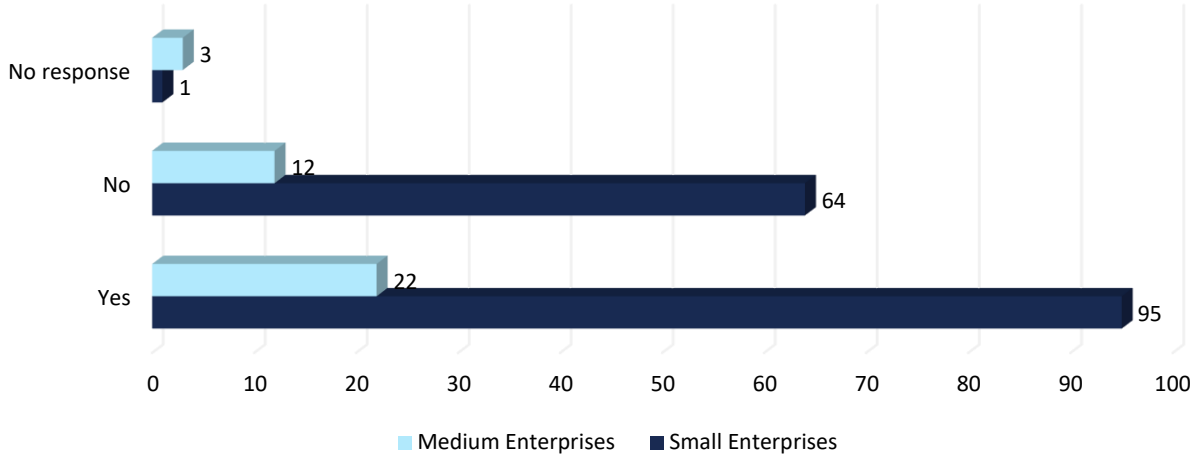


Source: IBC Advisory S.A. analyses based on CAWI survey.

The majority of respondents believe that development barriers can be overcome at the enterprise level. This view was expressed by 100 small and 20 medium-sized companies. In contrast, a total of 72 respondents disagreed - 58 from the small business sector and 14 from medium-sized enterprises. These results indicate that despite existing challenges, a significant number of companies see the potential to overcome development obstacles through internal actions, without the need for external support.

The chart below presents the opinions of cybersecurity sector representatives regarding the role of the state in overcoming development barriers. The data helps determine the extent to which entrepreneurs trust their own capabilities and market mechanisms, versus the degree to which they expect institutional and systemic support in addressing barriers that hinder growth.

Chart 37. In your opinion, can development barriers be overcome without state intervention? (N=197)

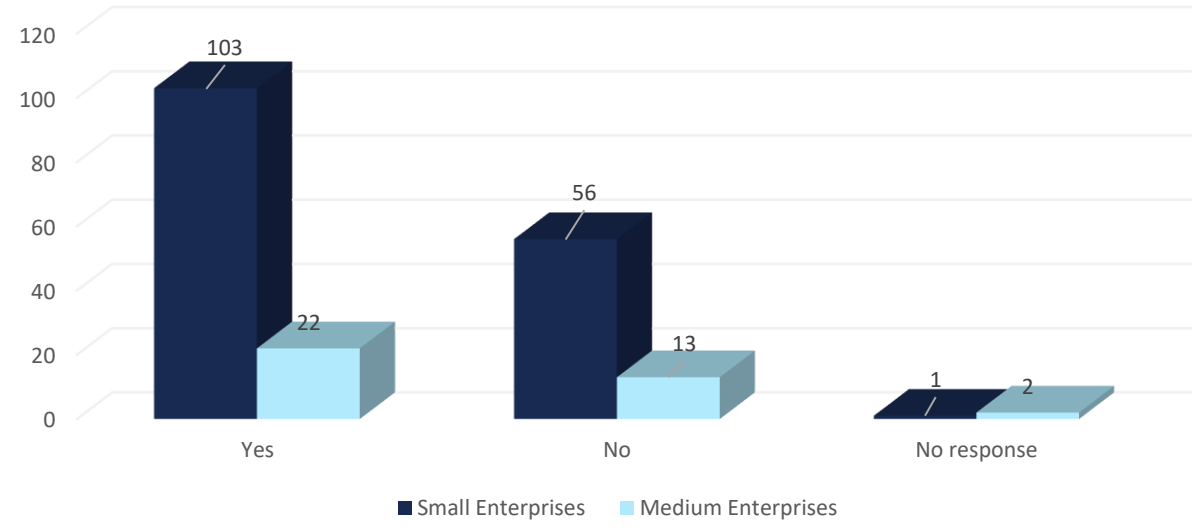


Source: IBC Advisory S.A. analyses based on CAWI survey.

The majority of respondents believe that development barriers can be overcome without the need for government intervention. This opinion was expressed by a total of 117 companies - 95 small and 22 medium-sized enterprises. In contrast, 76 respondents (64 small and 12 medium-sized companies) held the opposite view. These figures suggest that a significant proportion of firms see the potential to overcome barriers independently, although a notable group still perceives the need for support from public institutions.

In addition, respondents were asked for their views on the potential of artificial intelligence in addressing development barriers within companies. This analysis helps to understand the extent to which entrepreneurs recognize the role of AI in process optimization, automation, decision-making, and increasing operational efficiency.

Chart 38. In your opinion, can artificial intelligence contribute to overcoming development barriers? (N=197)



Source: IBC Advisory S.A. analyses based on CAWI survey.

Most respondents believe that artificial intelligence can help overcome development barriers. A total of 125 companies expressed this opinion - 103 small and 22 medium-sized enterprises. A contrary view was shared by 69 respondents (56 small and 13 medium companies). These results point to an awareness of AI's potential in supporting company growth, although a portion of businesses remain skeptical about its effectiveness.

The State as a Catalyst - The Expected Support Model

Paradoxically, despite a clear need for government intervention, many entrepreneurs are wary of the concept of "interventionism" itself. Their expectation is not for the state to replace the market, but rather to create conditions that enable fair competition and development.

> *"It's not that the state should do our work for us. But when we're competing with companies politically, legally, and financially supported by their governments, we at least need a level playing field."*

What is needed is partnership - the state as a catalyst for innovation, an initiator of joint initiatives, and a promoter of local expertise, not as a controller or top-down decision-maker.

Companies cannot overcome all barriers alone. For the Polish cybersecurity sector to realistically compete with global leaders, a deliberate, long-term national policy is needed - one that includes not only financing and certification but also export promotion, educational support, public procurement preferences, and a shift in the narrative around the notion of "Polish technology."

The Need for Systemic Support and an Industrial Strategy

As emphasized by all interviewees, Poland has the potential to become a significant player in cybersecurity. But without institutional backing, a smart industrial policy, and an effective strategy to build trust in domestic solutions, companies will continue to operate on the margins of global value chains - acting as subcontractors rather than innovation leaders.

The assessment of state activity in supporting the Polish cybersecurity sector - though partly positive - still raises a number of concerns and unmet expectations. Among industry representatives, there is both cautious optimism and disappointment, depending on the depth, effectiveness, and accessibility of government actions. Collected statements clearly show that while the level of dialogue between the administration and the sector has improved in recent years, many industry needs remain unaddressed.

Dialogue with the Administration: Progress and Limitations

Some respondents noted positive developments in engagement with public authorities. Entrepreneurs pointed out that state institutions are more frequently initiating consultations and meetings, and that cybersecurity is gaining prominence on the public agenda. One company representative, emphasizing the importance of concrete support instruments, especially those related to certification and product development, said:

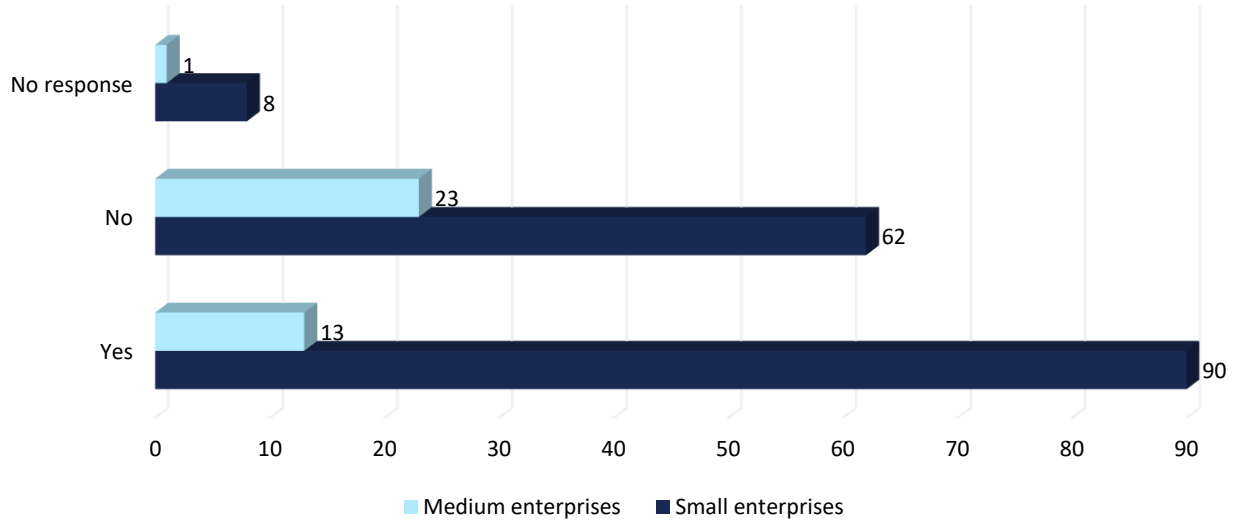
> *"I definitely appreciate the dialogue that's being held between the government and companies in this cybersecurity ecosystem. You can clearly see the openness, the willingness to meet and to talk. [...] Creating a program for the development of cybersecurity products and certifications was certainly valuable. [...] The idea itself is excellent, but it needs to be scaled up." ~ Respondent 4.*

For some companies, such initiatives represent an important step toward improving competitiveness in the European and global markets.

Ineffectiveness and Fragmentation of State Activities

The following chart presents respondents' assessments regarding the effectiveness of actions taken to develop the cybersecurity market in Poland. The responses help determine whether legislative, institutional, or financial initiatives are aligned with the sector's needs, and where significant gaps may still require improvement.

Chart 39. Do you believe that actions taken regarding the cybersecurity market require improvement? (N=197)



Source: IBC Advisory S.A. analyses based on CAWI survey.

Most respondents believe that actions taken to support the cybersecurity market require improvement. A total of 103 companies expressed this opinion - 90 small and 13 medium-sized enterprises. An opposing view was held by 85 firms (62 small and 23 medium companies). A small number of respondents (8 small and 1 medium-sized enterprise) declined to answer. These results indicate a clear expectation for enhancing existing mechanisms and initiatives in the field of cybersecurity.

However, despite some positive assessments, many respondents voiced strong concerns about the effectiveness and transparency of government actions. A recurring criticism was that support is often declarative or promotional in nature, rather than operational. Specific issues mentioned included the limited scale of available programs, lack of transparency in selection criteria, and lengthy, burdensome application procedures.

> *"[...] The Ministry of Digital Affairs - from my perspective - is a lot of marketing and very little action. [...] The consultation process has been completed [...] on the draft law regarding the national certification and cybersecurity system. Everyone - meaning the ministry and government - is praising it as a step in the right direction {…} We received information on how long it takes and what the costs are. I don't believe that if such a certification system is maintained, and if these costs amount to tens or even hundreds of thousands of PLN [...] it will be an expense that many of these companies simply cannot afford." ~ Respondent 9.*

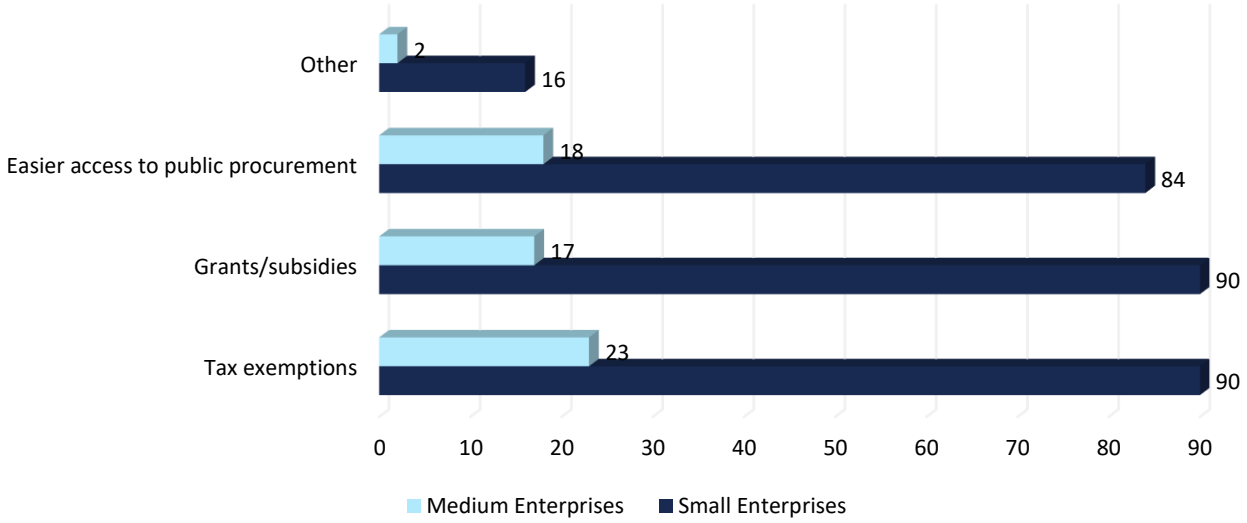
In this context, projects that claim to support Polish solutions but in practice promote foreign products and interests were especially criticized.

> *"[...] the PW Cyber initiative [...] sometimes gives me the impression that it's a bit dead or selective." ~ Respondent 4.*

The Need for Continuity and Structured Support Instruments

Chart 40 presents the expectations of cybersecurity firms regarding public actions that could most effectively support their development. The data shows that entrepreneurs place the highest importance on financial support in the form of tax relief and grants, but systemic actions are equally crucial - including easier access to public procurement, promotion of domestic solutions, and improved collaboration between government, academia, and industry.

Chart 40. Which public actions would be most helpful? (N=197)



Source: IBC Advisory S.A. analyses based on CAWI survey.

Among public actions considered most helpful by respondents, tax exemptions and grants/subsidies were the most frequently indicated, each receiving 90 mentions from small enterprises. Among medium-sized firms, 23 respondents pointed to tax exemptions, and 17 to grants and subsidies. The third most commonly cited measure was improved access to public procurement, with a total of 102 mentions (84 from small and 18 from medium enterprises).

An analysis of open-ended responses shows that companies expect not only financial support from the state, but primarily systemic and strategic involvement in the development of the domestic cybersecurity sector.

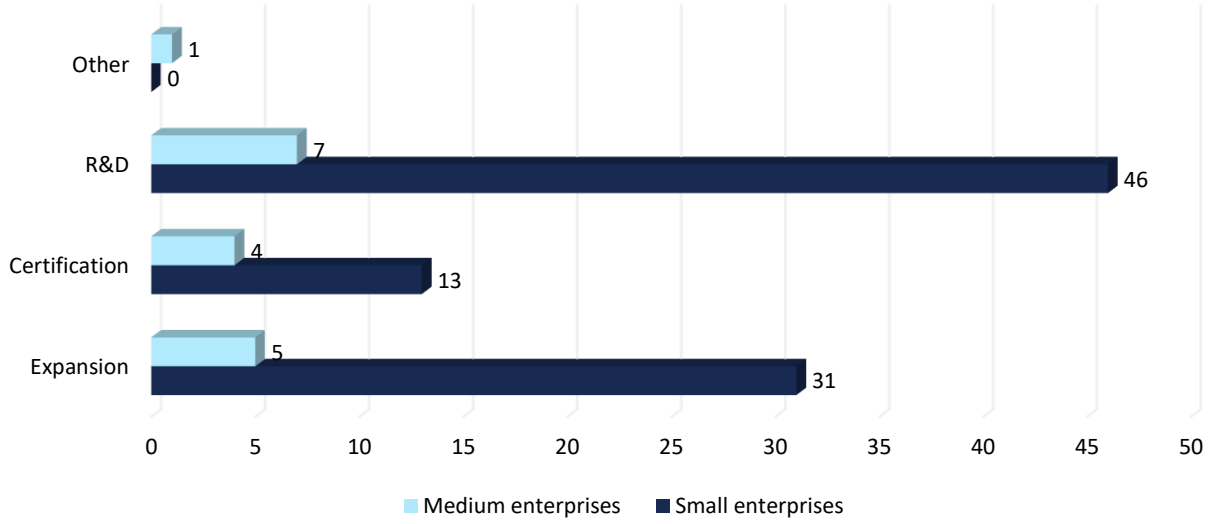
The most frequently mentioned postulates include:

1. Promotion and support for Polish tech companies - Respondents advocated for international promotion of domestic brands with state involvement, public relations and certification support, and institutional recommendations that encourage the use of local solutions.
2. Better institutional and legislative coordination - Respondents emphasized the need for increased awareness and competence within public administration, simplification of regulations (including tax laws), faster implementation of regulations (e.g., NIS2), and the creation of clear and effective mechanisms for inter-ministerial cooperation.
3. Building an ecosystem for science-business cooperation - Proposals included the mandatory involvement of private companies in R&D projects, the development of joint “use cases” with public administration, performance indicators for academic-industry collaboration, and support for clusters and business support institutions (e.g., funding participation in trade fairs, conferences, publications, etc.).
4. Regulatory and sectoral support - There were also demands for concrete infrastructural policies, such as preventing duplication of telecommunications networks and protecting small operators.

The need for traditional grant-based measures was mentioned less frequently - the emphasis has shifted toward long-term policies that support competitiveness and the international presence of Polish companies.

The following chart presents the preferences of cybersecurity companies regarding the allocation of public funds in the form of grants. The responses indicate that the highest priority is given to supporting R&D, international expansion, and certification processes - areas that are essential for innovation, competitiveness, and compliance with market requirements.

Chart 41. What types of activities should public grants support? (N=107)



Source: IBC Advisory S.A. analyses based on CAWI survey.

Respondents most frequently indicated that grants should be allocated to research and development (R&D) activities. This response was selected by a total of 53 companies - 46 small and 7 medium-sized enterprises. The second most important area was business expansion, indicated by 31 small and 5 medium companies. Certification was chosen as a priority by a total of 17 firms (13 small and 4 medium). The “other” category appeared in only one response, submitted by a medium-sized company. These results show that companies primarily expect support in innovation and growth, as well as in activities that facilitate entering new markets.

Responses to the question about the desired or sufficient amount of grant funding varied significantly. Some respondents gave specific figures, most commonly ranging from 1 to 10 million PLN. The lowest reported amounts were 3,000 PLN, 100,000 PLN, and 200,000 PLN (quoted both in PLN and EUR). Other values included 300,000 PLN per year, 500,000 PLN, and amounts between 1 and 2 million PLN (e.g., 1 million, 2 million, 2-5 million). There were also responses of 3 million, 6 million, and 10 million PLN, and a few even higher, such as “several million PLN,” “15-50 million,” or even 50 million PLN. Some responses were vague, mentioning “millions” or “x hundred thousand PLN.”

Several responses referred to grant size in percentage or conditional terms, e.g., as 10% of annual net profit, up to 50% of project value, within the limits of de minimis aid, or up to 200,000 PLN for companies with annual revenue below 1 million PLN. Some respondents noted that the level of support should depend on the type of project, its scale, or the specificity of the R&D sector. Others emphasized that the challenge lies not in the amount of funding itself but in the required co-financing and the instability of the institutional and political environment.

Respondents also expressed a need for better-designed, multi-stage support programs. The current model - based on one-time grants - is seen as insufficient, especially for companies needing continuous financing and a systemic growth model. As one respondent put it:

"The grant ends, the company collapses, and those people go on to get another grant. There's no continuity that way, especially when all this funding is supposed to go through Series A, B…"
~ Respondent 8

In this context, there were also calls for stronger promotion of European suppliers, especially in the area of public procurement - similar to how other countries support their national companies:

"[…] Provide support or a competitive advantage in public tenders for Polish enterprises. You can't really do this just for Polish companies, but I wonder if the EU as a whole shouldn't do more to favor European firms. And I don't mean American companies with a European branch, but truly European companies. […] In the United States, local firms are always favored. […] They're better perceived. Why shouldn't we do the same? I'd see this support more on a European scale, in terms of competitiveness, rather than just a Polish, local one." ~ Respondent 9.

The risk of losing digital sovereignty

Public funds allocated to the implementation of cybersecurity solutions - especially in public institutions such as hospitals - were positively assessed as an important investment impulse. However, significant concerns were also raised. A key issue is that these funds often end up going to foreign manufacturers, which in the long run may marginalize local companies and weaken Poland's digital sovereignty. As one respondent noted:

"[…] These grants made available to public institutions like hospitals - they don't really have the financial capacity to implement such solutions on their own. […] If it turns out that instead of using Polish-made solutions, American ones are implemented, that would be negative for us."
~ Respondent 10.

The Polish cybersecurity sector recognizes a number of barriers limiting its development, but at the same time demonstrates a high sense of agency. Most companies believe that many of these obstacles can be overcome at the enterprise level. They point to the potential of internal reorganization, innovation, investment in competencies, and new technologies. Among these solutions, artificial intelligence is playing an increasingly important role, with its implementation seen as a way to optimize processes and increase efficiency. AI is viewed as a tool supporting automation, data analysis, and decision-making. Nonetheless, many firms emphasize that systemic barriers-such as legal frameworks, taxes, or certification-require government intervention.

However, this is not about interfering with the free market, but rather about creating a level playing field. Entrepreneurs expect the state to act as a catalyst and partner, not as a regulator or owner. They point out that it is difficult to compete with companies subsidized by foreign governments without institutional support. They believe that Poland should-like the US, France, or Germany-promote and protect its domestic cybersecurity sector. They also call for a long-term industrial strategy and coordinated actions from public institutions.

While some respondents appreciate the improved dialogue with public administration, many point to a lack of transparency, insufficient scale of initiatives, and overly complex procedures. There is a prevailing sense that some public support programs are more declarative than operational. Companies complain about excessive paperwork, unclear criteria, and long decision-making timelines. They also criticize the lack of promotion for Polish products and the insufficient support for exports.

The most frequently demanded public measures include tax reliefs, grants, and easier access to public procurement. Entrepreneurs also call for simplified certification procedures and support for international promotion. They emphasize the need for better coordination between institutions and ministries, as well as improved collaboration between science and business. At the same time, they expect companies to be actively engaged in R&D projects and for infrastructure supporting the testing and implementation of solutions to be built.

Many respondents highlight the risk of marginalizing Polish companies if public support primarily benefits foreign suppliers. They warn that this could lead to loss of digital sovereignty and dependence on external technologies. They stress that the government should actively promote European and Polish solutions, particularly in public institutions. There is also a call for long-term development programs, not based on one-off grants, but on multi-stage financing models.

There is also a growing need to improve awareness of available support instruments. Many companies do not apply for funding due to a lack of knowledge, skills, or trust in the evaluation system. Additionally, they indicate that even the most advanced technological products cannot succeed without proper sales, promotional, and certification support. In this context, promoting startups and SMEs requires efforts to help them professionalize and scale.

Some companies are already actively using EU programs-such as *Horizon Europe* or *Digital Europe*-treating them as important development opportunities. Others are only now considering applying, noting that previous program offers were not well aligned with their profiles. Firms also call for local solutions to be promoted by the administration, through recommendations, participation in industry events, and PR support. A common theme across all voices is the expectation that the state will stop being a passive observer and become an active promoter of the sector.

In summary, cybersecurity firms show a strong willingness for self-driven growth, but they acknowledge the limits of what can be achieved without systemic support. To fully realize the sector's potential, it is essential to build a partnership-based ecosystem in which the state, business, and science cooperate in a coordinated, long-term, and transparent manner.

Bibliography

1. Artykuł ”Na czym polega ochrona danych osobowych RODO? Rozporządzenie RODO w pigułce”. EY, 2025.
2. Artykuł w portalu branżowym “Ekosystem rozwiązań cyberbezpieczeństwa w Polsce wart jest 12 mld zł.” ITwiz, 2024.
3. Artykuł w portalu branżowym “Poland Cybersecurity Market Size & Share Analysis – Growth Trends & Forecasts (2025–2030).” Mordor Intelligence.
4. Artykuł w portalu branżowym “Satus Starter VC zainwestował 2 miliony zł w Cybersecurity Studio”. MamStartup, 2021.
5. Artykuł w portalu branżowym „40 mln zł na cyberbezpieczeństwo od bValue. Fudo Security rozwinie skrzydła w USA.” XYZ, 2025.
6. Artykuł w portalu branżowym „Authologic z pomocą SMOK VC pozyskuje 8,2 mln dolarów na rozwój globalnej platformy weryfikacji tożsamości cyfrowej.” MyCompany Polska, 2022.
7. Artykuł w portalu branżowym „Biuro Informacji Kredytowej inwestuje w polski fintech Digital Fingerprints.” MamStartup, 2022.
8. Artykuł w portalu branżowym „Inwestycja 20 mln zł w Xopero.” CRN, 2024.
9. Artykuł w portalu branżowym „ResQuant z branży cybersecurity pozyskał finansowanie od Invento VC.” MamStartup, 2023.
10. Artykuł w portalu branżowym „To będą nowe polskie akceleratory. PARP ogłasza wyniki Startup Booster Poland – Smart UP.” MamStartup, 2024.
11. Artykuł “Bezpieczeństwo w chmurze”. Microsoft, 2025.
12. Artykuł “Building Trust for Today and Tomorrow”. PwC, 2025.
13. Artykuł “Co to jest zarządzanie dostępem i tożsamościami?”. Microsoft, 2025.
14. Artykuł “Cybersecurity Market Growth to Hit 15.9% CAGR Globally by 2030 – Exclusive Report by The Insight Partners.” GlobeNewswire, 8 Nov. 2023.
15. Artykuł “Digital Forensics and Incident Response Retainer Services Reviews and Ratings”. Gartner, 2025.
16. Artykuł “Network and Information Security Threat Landscape”. ENISA, 2023.
17. Artykuł “O SIlesia Smart Systems”, Silesia Smart Systems.
18. Artykuł “Penetration Testing and Red Teaming”. ENISA, 2023.
19. Artykuł “Security Awareness Training”. SANS Institute, 2025.
20. Artykuł “Szybka ścieżka – Innowacje cyfrowe (1/1.1.1/2022).” Narodowe Centrum Badań i Rozwoju.
21. Artykuł “Threat Landscape for Endpoint Security”. ENISA, 2023.
22. Artykuł “What Is a Security Operations Center (SOC)?”. IBM, 2024.
23. Artykuł “What Is Operational Technology (OT) Security?”. Cisco, 2025.
24. Artykuł „ORLEN VC z pierwszą polską inwestycją bezpośrednią.” PKN ORLEN, 2022.
25. Artykuł „Secfense pozyskuje 2 miliony dolarów w kolejnej rundzie inwestycyjnej.” Secfense, 2022.
26. Cybersecurity – Worldwide. Statista Market Forecast.
27. Dyrektywa (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (NIS2). Dz.U. L 333 z 27.12.2022.
28. Dyrektywa (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE. Dz.U. L 333 z 27.12.2022.
29. Informacja o firmie "DCD. Company. R&D", DCD, 2025.
30. Informacja o firmie "Perceptus. Projekty Unijne”, Perceptus, 2025.
31. Informacja o programie Fundusze Europejskie na Rozwój Cyfrowy 2021-2027.
32. Opis panelu „Szanse i Bariery dla MŚP działających w obszarze cyberbezpieczeństwa w Polsce” podczas Cybersec Forum w Katowicach, 2023 r. Gov.pl.

33. Publikacja “Vulnerability Management”. Qualys, 2023.
34. Raport “Polski rynek cyberbezpieczeństwa 2023–2028”. Polski Klaster Cyberbezpieczeństwa #CyberMadeInPoland, Październik. 2023.
35. Rozporządzenie (UE) 2019/881 w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych. Dz.U. L 151 z 07.06.2019.,
36. Rozporządzenie (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego oraz zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014 i (UE) 2019/2033. Dz.U. L 333 z 27.12.2022.,
37. Rozporządzenie (UE) 2024/2847 z dnia 12 marca 2024 r. w sprawie horyzontalnych wymagań dotyczących cyberbezpieczeństwa dla produktów z elementami cyfrowymi oraz zmieniające rozporządzenie (UE) 2019/1020. Dz.U. L 333 z 27.12.2024.
38. Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024. Ministerstwo Cyfryzacji, 2019.
39. Strona internetowa firmy „Atende inwestuje w Cryptomage – spółkę łączącą AI z cyberbezpieczeństwem sieciowym.” Atende, 2023.
40. Strona internetowa firmy „Techstep acquires software company Famoc, adding MMS capabilities.” Techstep, 10 maja 2021.
41. Strona internetowa PAIH “O projekcie – Polskie Mosty Technologiczne.” Polska Agencja Inwestycji i Handlu (PAIH).
42. Strona internetowa PARP “Go to Brand.” Polska Agencja Rozwoju Przedsiębiorczości (PARP).
43. Strona internetowa PFR “Dla działań wspierających rozwój technologii o potencjale podwójnego przeznaczenia”. Polski Fundusz Rozwoju S.A., 2024.
44. Strona internetowa Instytutu Łączności – Państwowego Instytutu Badawczego, Gov.pl.
45. Strona internetowa Łukasiewicz – AI, Gov.pl.
46. Strona internetowa Ministerstwa Cyfryzacji - Działania, Gov.pl.
47. Strona internetowa Ministerstwa Rozwoju i Technologii - działania ministerstwa, Gov.pl.
48. Strona internetowa Narodowego Centrum Badań i Rozwoju, Gov.pl.
49. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Dz.U. 2018, poz. 1560.
50. Wpis na stronie kancelarii prawnej „We advised CyCommSec.” LLW Lewczuk Łyszczarek Szymczyk, 2025.
51. Wpis w portalu branżowym „Asseco Poland kupiło 69,01% akcji spółki ComCERT.” Money.pl, 2019.
52. Założenia programu B+R CyberSecIdent: Cyberbezpieczeństwo i eTożsamość, aktualizacja nr 4. Narodowe Centrum Badań i Rozwoju.

List of Charts and Figures

Charts

Chart 1. *What is the size category of the enterprise? (N=197)* 20
Chart 2. *Types of Business Activity in the Cybersecurity Sector (N=197)* 21
Chart 3. *How many years has the company been operating in the market? (N=197)* 22
Chart 4. *How many years has the company been active in the field of cybersecurity? (N=197)* 22
Chart 5. *Type of company ownership: (N=197)* 23
Chart 6. *Is your company a member of any industry organization (e.g. cluster, chamber of commerce)? (N=197)* 24
Chart 7. *What technologies/services are being developed by your company? (N=197)* 26
Chart 8. *What is the company's annual revenue range? (N=197)* 28
Chart 9. *Do you offer your products as cloud services, on-premise solutions, or in a hybrid model? (N=197)* 29
Chart 10. *Do you use sales intermediaries such as integrators, distributors, or resellers? (N=197)* 29
Chart 11. *Do you offer products/services/technologies developed by other domestic companies? (N=51)* 30
Chart 12. *How would you rate the professional potential of your staff? (N=197)* 34
Chart 13. *Which roles listed in the European Cybersecurity Skills Framework (ECSF) are present in your company? (N=197)* 35
Chart 14. *Have you experienced difficulties in hiring adequately qualified employees in the past year? (N=197)* 36
Chart 15. *Do you plan to make investments in the coming year? (N=197)* 43
Chart 16. *Do the planned investments concern R&D infrastructure? (N=96)* 44
Chart 17. *Are you planning to expand your operations? (N=197)* 45
Chart 18. *Have you used the services of technology accelerators or incubators? (N=197)* 47
Chart 19. *Is there knowledge within your company about the certification process? (N=197)* 49
Chart 20. *Do you have plans to certify your products/services? (N=197)* 49
Chart 21. *Does your company hold any patents/licenses/trademarks/utility models, etc., related to your products/services? (N=197)* 50
Chart 22. *Number of certifications/accreditations/quality approvals (N=71)* 51
Chart 23. *How many patents/licenses/trademarks/utility models, etc., related to your products/services does your company hold? (N=69)* 52
Chart 24. *Has your company previously used national or EU support to foster development (e.g., R&D projects)? (N=197)* 53
Chart 25. *What was the reason for not using this type of support (e.g., development or R&D projects)? (N=152)* 53
Chart 26. *Has the company previously used national or EU support to expand its operations in the cybersecurity sector? (N=197)* 54
Chart 27. *What was the reason for not using this form of support (business expansion)? (N=153)* 55
Chart 28. *Is your company familiar with EU programs supporting product/service development (e.g., Horizon Europe, FENG, Digital Europe)? (N=197)* 57
Chart 29. *Has your company received support from private financing sources (e.g., venture capital, private equity) in the past 3 years? (N=197)* 59
Chart 30. *If not, what was the reason? (N=156)* 59
Chart 31. *What is the geographic scope of your company's operations? (N=197)* 64
Chart 32. *Does your company face any development barriers? (N=197)* 68
Chart 33. *If you do not plan to expand your operations, what is the main reason? (N=70)* 69
Chart 34. *What are the most significant development challenges currently facing your company? (N=49)* 70
Chart 35. *Are you familiar with the CRA and NIS2 regulations? (N=197)* 78
Chart 36. *In your opinion, can development barriers be overcome at the enterprise level? (N=197)* 83
Chart 37. *In your opinion, can development barriers be overcome without state intervention? (N=197)* 84
Chart 38. *In your opinion, can artificial intelligence contribute to overcoming development barriers? (N=197)* 84
Chart 39. *Do you believe that actions taken regarding the cybersecurity market require improvement? (N=197)* 86
Chart 40. *Which public actions would be most helpful? (N=197)* 87
Chart 41. *What types of activities should public grants support? (N=107)* 88

Maps

Map 1. *Geographic Distribution of Cybersecurity Companies* 16

Figures

Figure 1. *Cooperative Links* 66

The report *"Map of Cybersecurity SMEs in Poland: Diagnosis, Needs, Recommendations"* is an original publication by IBC Advisory S.A., prepared by IBC experts at the request of the Minister of Digital Affairs.

Citation: Kołodziej E., Grzęda Ł., Gawron Ł., Pardyak O., Kamińska E., Wojtyczek K., Kolorz R., Jacak P. (2025). *Map of Cybersecurity SMEs in Poland: Diagnosis, Needs, Recommendations*, IBC Advisory S.A., Warsaw.

Contact:
ibc@ibc-advisory.pl

Autors
Emilian Kołodziej
dr Łukasz Grzęda
Łukasz Garwon
Oskar Pardyak
Ewa Kamińska
Karolina Wojtyczek
Rafał Kolorz
Paweł Jacak

Prepared by:

IBC Advisory Spółka Akcyjna

Editorial Team

Ewa Kamińska
Oskar Pardyak

Expert Contribution

Polski Klaster Cyberbezpieczeństwa #CyberMadeInPoland

Graphic Design and Layout

Krystian Ścipień

Warsaw, 2025

All data and projections included in this publication are based on primary research and the latest data from public databases and registers. The work carried out by IBC in the development of this report consisted of a comprehensive analysis of the Polish small and medium-sized enterprise (SME) sector operating in the cybersecurity industry. These analyses were used in their original form to support the mapping of the Polish SME cybersecurity sector.

This report was prepared by IBC consultants commissioned by the Ministry of Digital Affairs. It has been compiled with due diligence; however, certain information may have been presented in a summarized or general form. The publication is for informational purposes only. The data it contains should not replace professional advice when making investment decisions.

IBC provides data for the design and evaluation of public policies and interventions. We support strategic initiatives of ministries, major public sector institutions, and business leaders in Poland's key economic sectors, especially those aligned with smart specialization strategies. The data we collect is analyzed using advanced statistical applications and project-specific algorithms. Using our proprietary data collection and analytics methodology, we have developed a research offering that enables access to insights and data on beneficiaries, consumers, and 27 EU markets.

| Social and Evaluation Research | Data Analytics | Econometric Modeling | Economic Research

www.ibc-advisory.pl

NCC-PL National Cybersecurity Coordination Centre Poland

Ministry of Digital Affairs Republic of Poland

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE