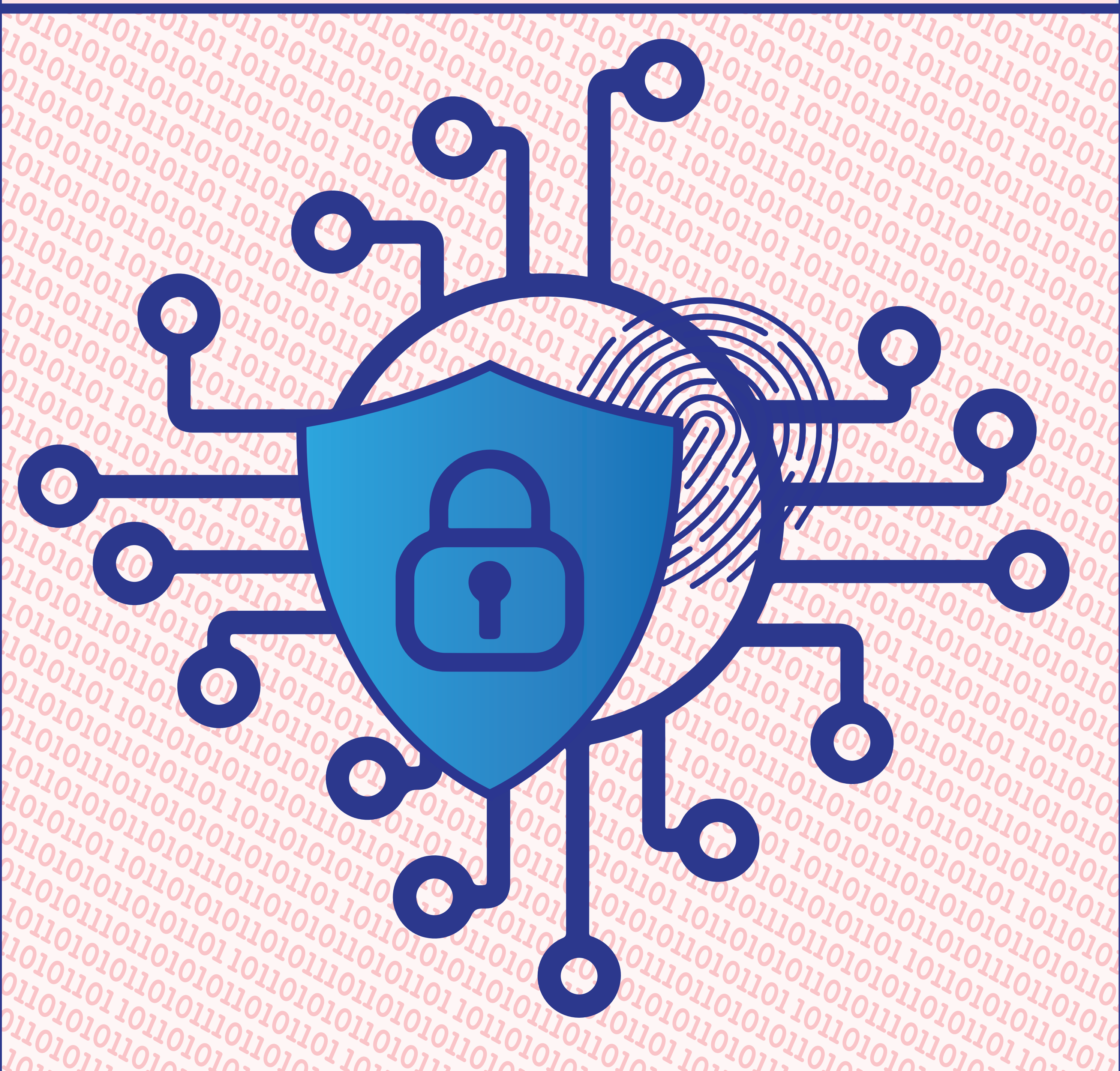
The 2023 Luxembourg cybersecurity ecosystem study

May 2024



nc3
Cybersecurity Observatory

nc3.lu
National Cybersecurity
Competence Center
LUXEMBOURG

ABOUT NC3

The National Cybersecurity Competence Center (NC3) is Luxembourg's focal point for cybersecurity initiatives and capabilities. The NC3 is one of the two hosted centres of the Luxembourg House of Cybersecurity with CIRCL (Computer Incident Response Center Luxembourg). Established in 2023, NC3 plays an instrumental role in fortifying the nation's cybersecurity posture. The center collaborates with public and private sector entities to develop and implement strategies aimed at bolstering cybersecurity defenses. From threat intelligence to research and development, NC3 works diligently to address current cyber risks while anticipating future challenges. Through knowledge dissemination, skill-building, and public awareness, the center aims to secure Luxembourg's digital assets and critical infrastructure. For further information about NC3 and its initiatives, visit: https://nc3.lu/

CONTACT

To get in touch with the experts, please use: contact@nc3.lu
For media inquiries, please email: communication@lhc.lu

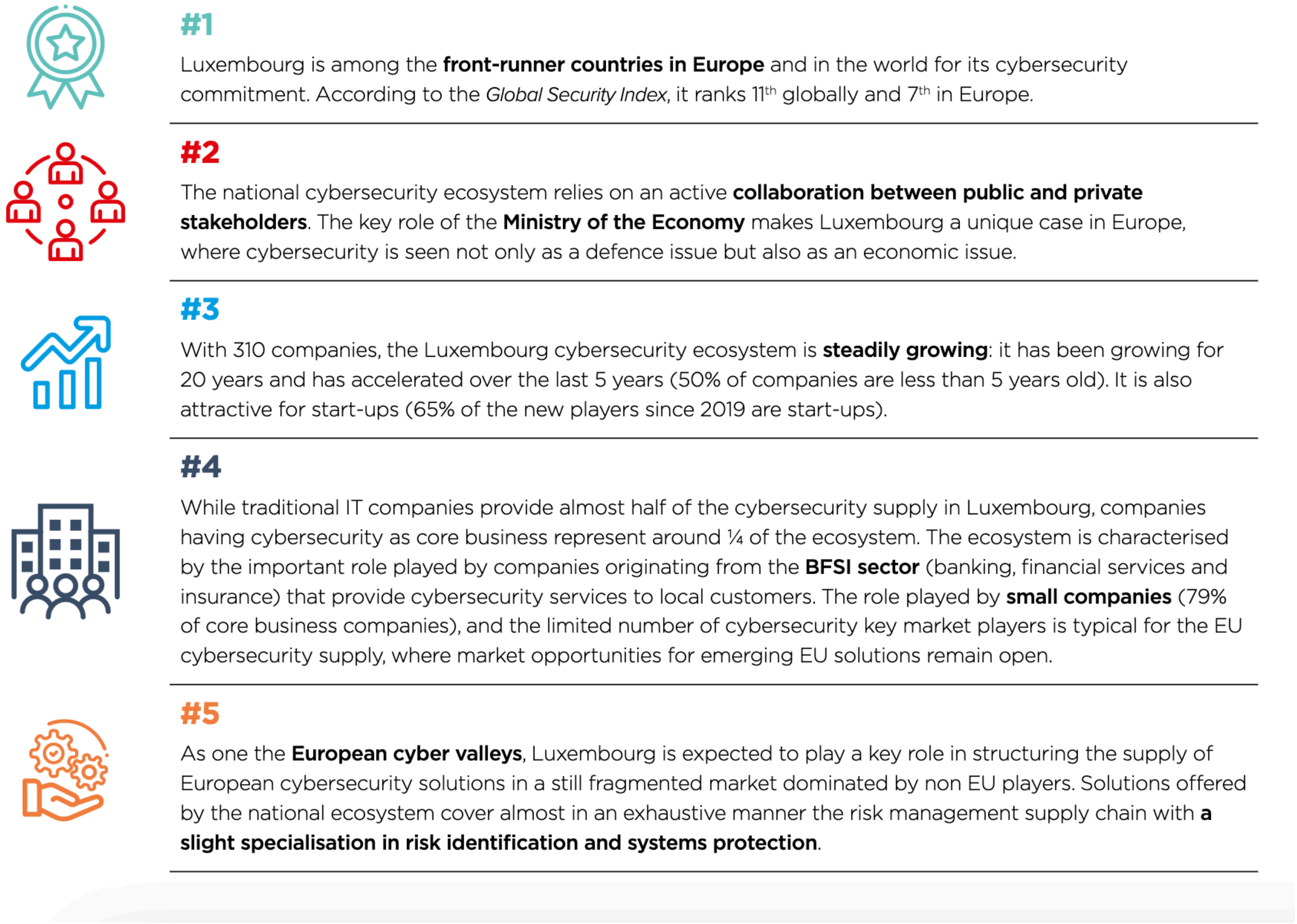
ACKNOWLEDGEMENTS

Our warmest thanks go to all participating experts from the Chambre of Commerce, the private companies #mans, Conostix, Excellium, Innov'ICTion, and Telindus and to all the other organizations who helped us to gather insights about the market. We also extend our gratitude to the Ministry of the Economy of Luxembourg, our colleagues of the Luxembourg House of Cybersecurity and all the cybersecurity solution providers that participated in our survey and focus group for their invaluable contributions to the mission of the National Cybersecurity Competence Center.

Table of Contents

Executive summary

The 2023 cybersecurity ecosystem study builds upon previous analyses conducted by Luxinnovation (LXI) in partnership with the Luxembourg House of Cybersecurity (LHC). With the establishment of the market intelligence observatory platform within the LHC, the National Cybersecurity Competence Center (NC3) has embarked on a series of studies aimed at addressing the varied needs of stakeholders in the cybersecurity market. The inaugural study, titled "A Comprehensive Market Study on Cybersecurity Challenges and Opportunities in Luxembourg's SME sector,"[1] lays the groundwork for this endeavor. Our study is informed by critical insights from the LXI-Market Intelligence report,[2] which examined 2020 data from the national ecosystem, supplemented by additional external sources. The following list summarizes the key insights from the LXI-Market Intelligence report from 2020.



#1

Luxembourg is among the **front-runner countries in Europe** and in the world for its cybersecurity commitment. According to the *Global Security Index*, it ranks 11th globally and 7th in Europe.

#2

The national cybersecurity ecosystem relies on an active **collaboration between public and private stakeholders**. The key role of the **Ministry of the Economy** makes Luxembourg a unique case in Europe, where cybersecurity is seen not only as a defence issue but also as an economic issue.

#3

With 310 companies, the Luxembourg cybersecurity ecosystem is **steadily growing**: it has been growing for 20 years and has accelerated over the last 5 years (50% of companies are less than 5 years old). It is also attractive for start-ups (65% of the new players since 2019 are start-ups).

#4

While traditional IT companies provide almost half of the cybersecurity supply in Luxembourg, companies having cybersecurity as core business represent around ¼ of the ecosystem. The ecosystem is characterised by the important role played by companies originating from the **BFSI sector** (banking, financial services and insurance) that provide cybersecurity services to local customers. The role played by **small companies** (79% of core business companies), and the limited number of cybersecurity key market players is typical for the EU cybersecurity supply, where market opportunities for emerging EU solutions remain open.

#5

As one the **European cyber valleys**, Luxembourg is expected to play a key role in structuring the supply of European cybersecurity solutions in a still fragmented market dominated by non EU players. Solutions offered by the national ecosystem cover almost in an exhaustive manner the risk management supply chain with **a slight specialisation in risk identification and systems protection**.

Figure 1: key insights of the CYBERSECURITY Luxembourg study of 2020

[1] A Comprehensive Market Study on Cybersecurity Challenges and Opportunities in Luxembourg's SME sector, Last Accessed: 23/01/2024 Link: https://observatory.nc3.lu/market-intelligence-library/report-2023/

[2] Luxembourg Cybersecurity Ecosystem – Key Insights (2020), Source: Luxinnovation, Last Accessed: 15/11/2023, Link: https://www.luxinnovation.lu/fr/publication/luxembourg-cybersecurity-ecosystem-key-insights-2020

This foundational report was pivotal in showcasing the growth of the ecosystem and providing an overarching view of Luxembourg's position in the global cybersecurity arena. The study's scope was further enhanced by a recent Threat Landscape analysis conducted by LHC, yielding valuable information on current trends and incidents.

Key highlights of the Luxembourg cybersecurity ecosystem study 2023:

1. Strategic evolution into a cybersecurity hub: Over the past two decades, Luxembourg has significantly advanced its cybersecurity infrastructure, in alignment with the OECD's guidelines in terms of awareness, education, risk management, collaboration, and legal framework.. The cybersecurity sector has evolved into a cornerstone of national development and economic growth.
2. Recognition in Global Cybersecurity Index (GCI): Luxembourg ranks highly in Europe for cybersecurity measures, with achievements in legal, technical, and cooperative aspects, and potential for further improvement in organizational measures.[3]
3. CYBERSECURITY Luxembourg initiative: Launched in 2019, this initiative fosters public-private cooperation, aligning with the national cybersecurity strategy. A comprehensive mapping and interactive dashboard enhance sector visibility and collaboration.[4]
4. Market dynamics and financial analysis: The European cybersecurity market is expected to grow significantly, driven by digital transformation, IoT, and emerging cyber risks. A detailed financial analysis of Luxembourg's cybersecurity sector reveals disparities among companies and a concentration of smaller-sized entities.
5. Public services and government role: There's an expectation for increased government support in bolstering Luxembourg's cybersecurity ecosystem, focusing on private-public partnerships, support for security SMEs, and funding and incentives.
6. Sector-specific approach and market trends: Financial and insurance activities are the most targeted sectors by cyberattacks. The cybersecurity market, on the other side, is characterized by diverse revenue-generating activities and a mixed approach towards open-source solutions and innovation.
7. Market strengths and weaknesses: Strengths include strong demand from the financial sector and Luxembourg's international orientation. Weaknesses encompass high cost of living and limited market size.
8. Future concerns and opportunities: Major concerns include human resources shortages and remote work constraints. Opportunities lie in enhancing government support and pro-

[3] Global Cybersecurity Index 2020, Source: ITU, Last Accessed: 23/01/2024, Link: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

[4] The Ecosystem Dashboard, Source: CYBERSECURITY Luxembourg, Last Accessed: 23/01/2024, Source: https://cybersecurity.lu/dashboard

moting local cybersecurity companies.

Conclusion and future directions:

The study validates the varying levels of cybersecurity maturity among SMEs and highlights the crucial role of human resources in the sector. The emphasis on talent acquisition, retention, and development is pivotal for the effectiveness of digital and cybersecurity strategies. Future research will focus on bridging the skills shortage in cybersecurity, enhancing organizational postures, and preparing for evolving cybersecurity workforce demands.

The NC3's ongoing commitment to this research reflects its dedication to strengthening Luxembourg's position as a leading cybersecurity hub, ready to face the challenges of a digital future.

A comprehensive Market Study on Luxembourg's cybersecurity ecosystem in 2023

1 – Positioning of Luxembourg as a cybersecurity hub

1.1 – Luxembourg's strategic evolution into a cybersecurity hub

Cybersecurity plays a crucial role in Luxembourg's efforts to foster all facets of digital transformation and build a data-driven economy.[5] Over the past two decades, the country has significantly advanced its infrastructure in this domain. Guided by the Ministry of the Economy and adhering to the OECD's 'Towards a Culture of Security' guidelines,[6] Luxembourg has made substantial investments in cybersecurity such as the creation of dedicated agencies to support the private sector, LHC, and specific topics like cryptography, INCERT.[7] This effort has led to the creation of a robust, active, and expanding cybersecurity ecosystem. The sector, which intersects with various industries, has evolved into a cornerstone of Luxembourg's national development strategy and economic growth. Cybersecurity plays a crucial role in Luxembourg's endeavor to foster all facets of digital transformation and to build a data-driven economy. The digital revolution is changing business practices, enabling enhanced functionality and the provision of solutions with unparalleled speed and adaptability. This implies that Luxembourg recognizes the importance of adapting to these changes and leveraging digital transformation, while also prioritizing cybersecurity to ensure the safety and protection of digital assets and data. To structure this approach and remain up-to-date with the rapid pace of digital technologies and practices, the Luxembourg government has published several national cybersecurity strategies in alignment with other European member states and recommendations from the European cybersecurity agency, ENISA, as shown below.

[5] The data-driven innovation strategy for the development of a trusted and sustainable economy in Luxembourg, Source: The Government of the Grand Duchy of Luxembourg – Ministry of the Economy, Last Accessed: 23/01/2024, Link: https://gouvernement.lu/dam-assets/fr/publications/rapport-etude-analyse/minist-economie/The-Data-driven-Innovation-Strategy.pdf

[6] OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, Source: Organisation for Economic Co-operation and Development, Last Accessed: 15/11/2023, Link: https://www.oecd.org/sti/ieconomy/oecdguidelinesforthesecurityofinformationsystemsandnetworkstowardsacultureofsecurity.htm

[7] Historical missions of INCERT, Source: INCERT, Last Accessed: 23/01/2024, Link: https://www.incert.lu/#missions

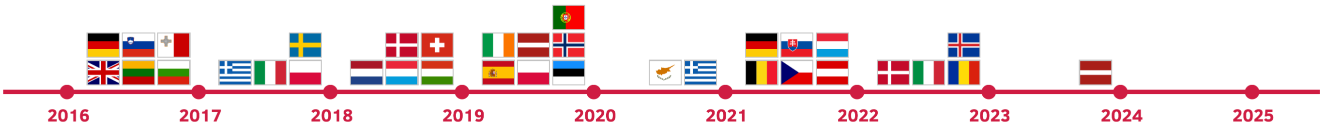
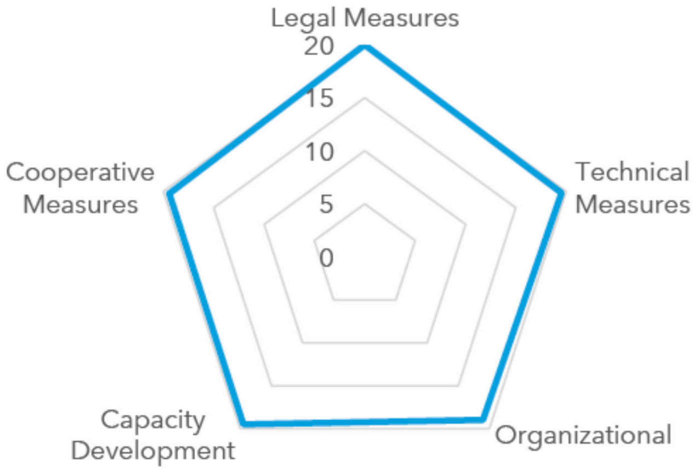


Figure 2: Country strategies released per year listed by ENISA[8]

1.2 – Fast pace race for cybersecurity maturity

The Luxembourg cybersecurity ecosystem's development has been recognized in the Global Cybersecurity Index (GCI), released by the International Telecommunication Union (ITU), a specialized United Nations agency overseeing information and communication technology matters. In 2018,[9] Luxembourg ranked 7th in Europe and 11th globally. Although its global ranking slipped to 13th in the 2020 edition[10] of the GCI, Luxembourg achieved a higher score of 97.41, maintaining its position within Europe. These scores, as illustrated by the following chart, indicate that Luxembourg has achieved a substantial level of maturity in its cybersecurity measures, particularly in legal, technical, and cooperative aspects, with limited scope for further enhancement in these areas, though there remains some potential for improvement in organizational measures.



Development Level:
Developed Country,
Landlocked Country

Area(s) of Relative Strength
Legal, Technical Measures
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
97.41	20.00	19.54	18.98	19.48	19.41

Figure 3: Luxembourg's profile in the GCI 2020

[8] National Cyber Security Strategies – Interactive Map, Source: ENISA, Last Accessed: 15/11/2023, Link: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map

[9] Global Cybersecurity Index 2018, Source: ITU, Last Accessed: 15/11/2023, Link: http://handle.itu.int/11.1002/pub/813559ed-en

[10] Global Cybersecurity Index 2020, Source: ITU, Last Accessed: 15/11/2023, Link: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

1.3 – Luxembourg's national strategy and inter-ministerial coordination efforts

In December 2017, the Luxembourg Government established an inter-ministerial committee, led by the High Commissioner for National Protection, to coordinate national cybersecurity efforts. This committee comprises representatives from key state entities in cybersecurity. Prime Minister Xavier Bettel introduced Luxembourg's fourth national cybersecurity strategy for 2021-2025, highlighting the government's response to the dynamic digital environment. The strategy was formulated by a task force under the High Commissioner's leadership, including members from various state departments such as the State's Information Technology Centre, GOVCERT, ANSSI, and others, addressing a broad range of cybersecurity challenges. This strategy marks the first mention of the national cybersecurity ecosystem initiative, CYBERSECURITY Luxembourg.[11]

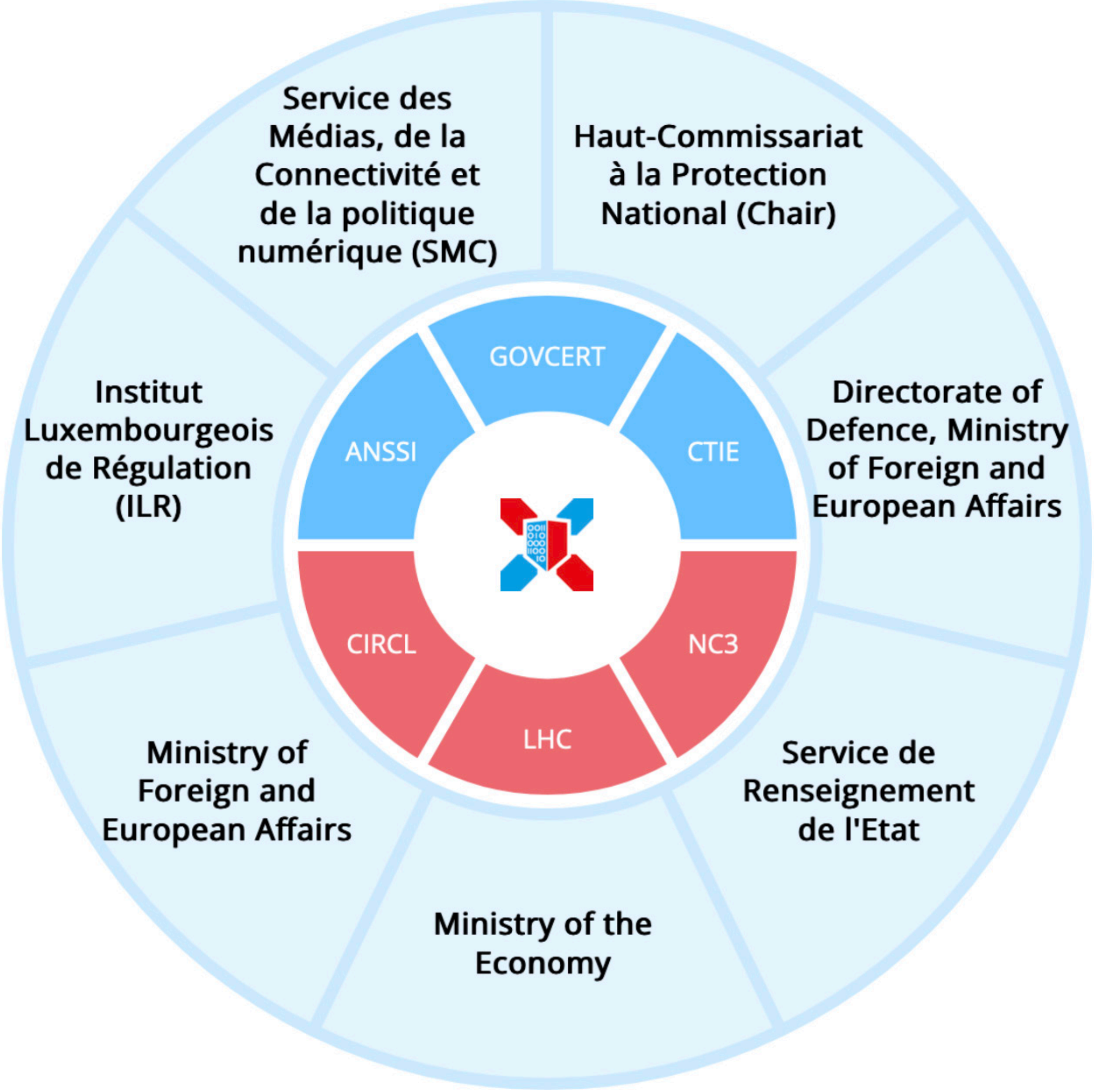

Service des Médias, de la Connectivité et de la politique numérique (SMC)
Haut-Commissariat à la Protection National (Chair)
Directorate of Defence, Ministry of Foreign and European Affairs
Service de Renseignement de l'Etat
Ministry of the Economy
Ministry of Foreign and European Affairs
Institut Luxembourgeois de Régulation (ILR)
GOVCERT
CTIE
NC3
LHC
CIRCL
ANSSI

Figure 4: Intermisterial Committee for Prevention and Cybersecurity (CIC-CPS)

[11] National Cybersecurity Strategy IV, Source: High Commission for National Protection, Last Accessed: 15/11/2023, Link: https://hcpn.gouvernement.lu/en/publications/strategie-nationale-cybersecurite-4/strategie-nationale-cybersecurite-4.html

1.4 – The CYBERSECURITY Luxembourg initiative and ecosystem mapping

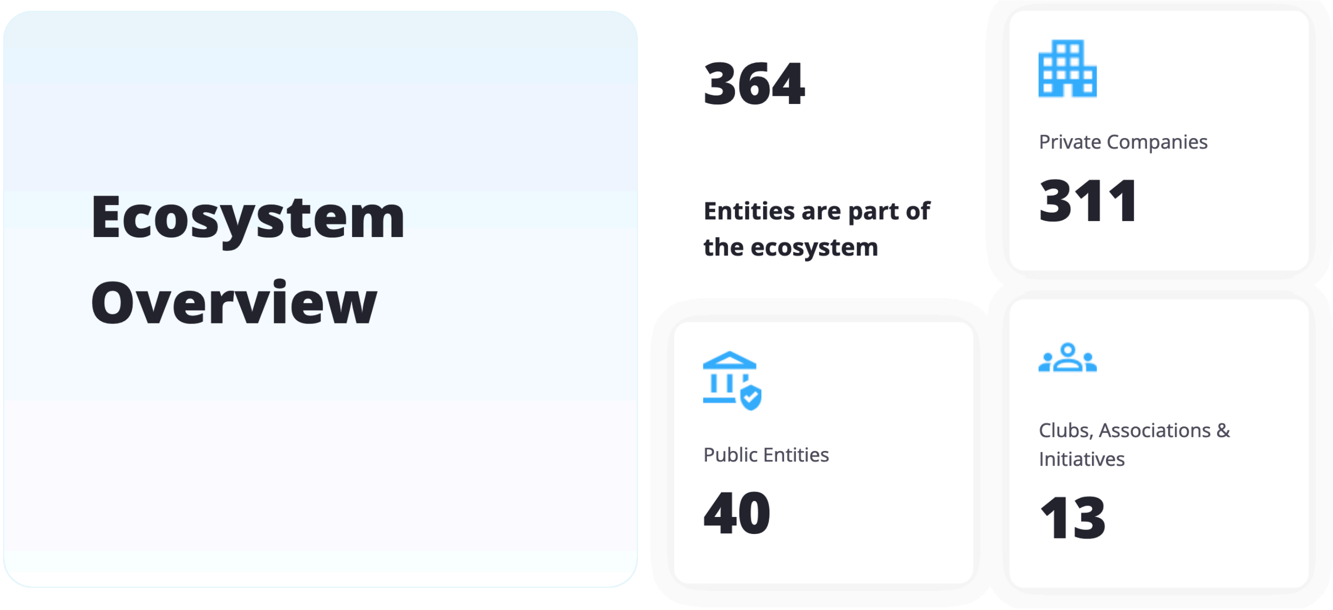
Under the high patronage of the Ministry of the Economy and initiated by Minister Étienne Schneider, the CYBERSECURITY Luxembourg initiative was launched in 2019 to strengthen public-private cooperation in cybersecurity, aligning with the national cybersecurity strategy. This initiative is spearheaded by prominent national cybersecurity stakeholders: the High Commissioner for National Protection (HCPN) and the Luxembourg House of Cybersecurity, previously known as SECURITYMADEIN.LU, with the support of Luxinnovation. The Luxembourg House of Cybersecurity introduced the concept of the cybersecurity ecosystem to highlight the local cybersecurity community, providing users with central and easy access to all relevant actors and initiatives of the Luxembourg cybersecurity ecosystem. Since its inception, the ecosystem has grown significantly.

To navigate this burgeoning landscape, a comprehensive map was needed. Luxinnovation and the Luxembourg House of Cybersecurity collaborated to create this map, enhancing the sector's visibility and clarifying the roles and activities of different players. This first mapping[12] was officially presented on October 14, 2019, at the National Cybersecurity Competence Center (NC3), attended by Deputy Prime Minister and Minister of the Economy, Étienne Schneider. It was followed in 2020 by an online interactive dashboard[13] updating the figures of the previous edition and allowing users to explore the data more in detail. Since 2021, the national cybersecurity ecosystem hosts the interactive dashboard on its own platform[14] which also allow to update the data directly from the input of the market players.

[12] Luxembourg cybersecurity ecosystem mapping 2019, Source: Luxinnovation, Last Accessed: 15/11/2023, Link: https://www.luxinnovation.lu/wp-content/uploads/sites/3/2019/10/luxembourg-cybersecurity-ecosystem_mapping-2019-1.pdf

[13] Luxembourg cybersecurity ecosystem mapping 2020, Source: Luxinnovation, Last Accessed: 15/11/2023, Link: https://app.powerbi.com/view?r=eyJrIjoiZDEzYzYwOTYtMTk0Yy00NTBkLWI3NjEtNTAwYWZiYTFmNzhhIiwidCI6ImRiNGE4Mjc4LWE3NjMtNGIzYS1hZjY3LWQ2MzE2NDVmYTRlMCIsImMiOjl9

[14] Luxembourg cybersecurity ecosystem dashboard, Source: CYBERSECURITY Luxembourg, Last Accessed: 15/11/2023, Link: https://www.luxinnovation.lu/wp-content/uploads/sites/3/2019/10/luxembourg-cybersecurity-ecosystem_mapping-2019-1.pdf



Ecosystem Overview

364

Entities are part of the ecosystem

Private Companies

311

Public Entities

40

Clubs, Associations & Initiatives

13

Figure 5: Luxembourg cybersecurity ecosystem dashboard as of November 21, 2023

CYBERSECURITY Luxembourg, as Luxembourg's cybersecurity ecosystem, consolidates and enhances public-private collaboration in cybersecurity. It operates as the national label for Luxembourg's cybersecurity efforts, uniting and aiding all relevant private and public sector entities. This collaboration aims to fortify this vital aspect of the national economy and promote Luxembourg's cybersecurity expertise globally.

1.5 – Luxembourg cybersecurity ecosystem sourcing methodology

The first CYBERSECURITY Luxembourg ecosystem mapping process began with Luxinnovation's Market Intelligence Team (LXI-Market Intelligence) developing a database to identify potential members of the cybersecurity ecosystem in Luxembourg, utilizing a range of data sources.

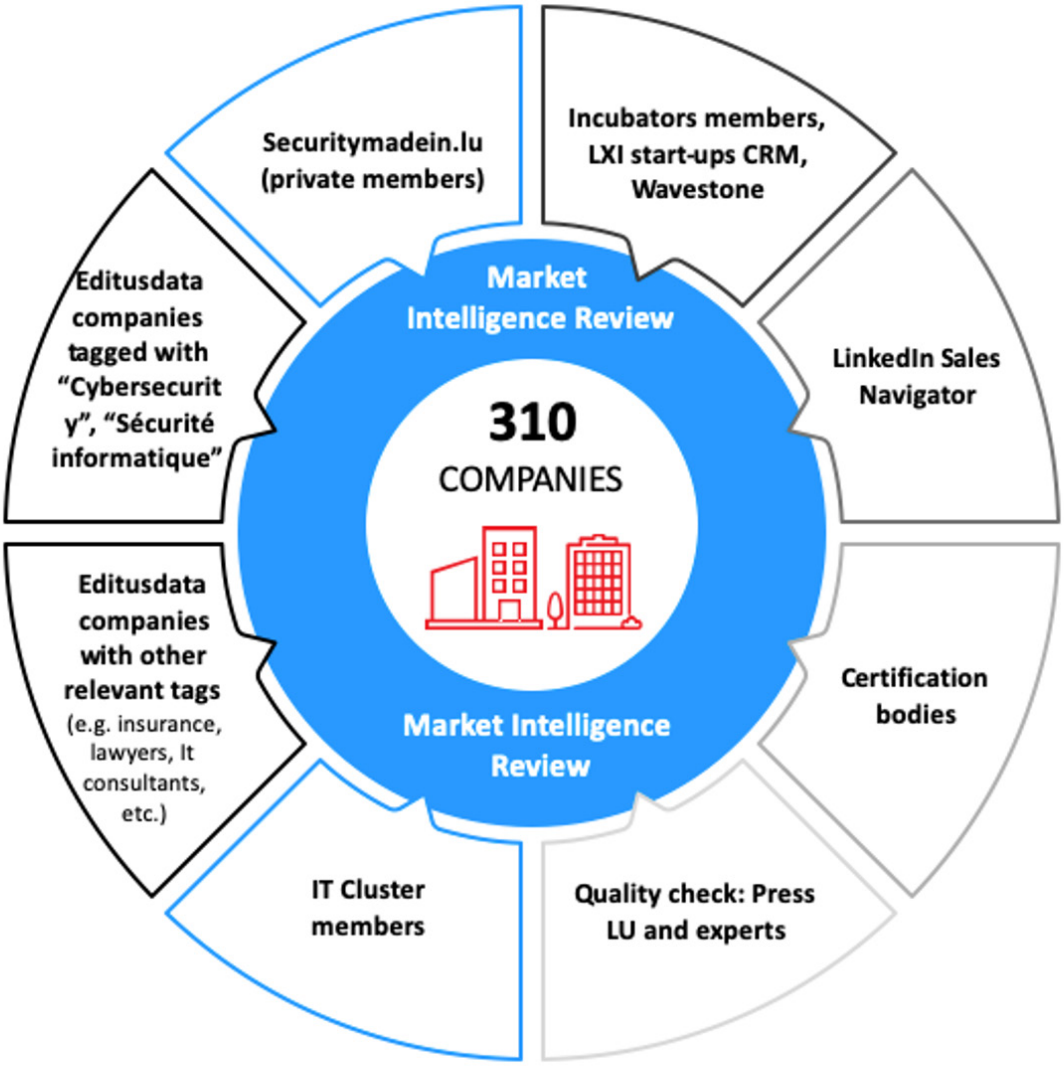

Securitymadein.lu (private members)
Incubators members, LXI start-ups CRM, Wavestone
LinkedIn Sales Navigator
Certification bodies
Quality check: Press LU and experts
IT Cluster members
Editusdata companies with other relevant tags (e.g. insurance, lawyers, It consultants, etc.)
Editusdata companies tagged with "Cybersecurit y", "Sécurité informatique"
Market Intelligence Review
310
COMPANIES
Market Intelligence Review

Figure 6: Data sources used by LXI-Market Intelligence for mapping market players

The potential members of the ecosystem were reviewed and classified by the Luxembourg House of Cybersecurity, using an approach inspired by the European Cyber Security Organisation (ECSO) market radar's taxonomy[15] and based on the classification of cybersecurity activities from the NIST Cybersecurity Framework.[16] The Core of this framework includes five main functions—Identify, Protect, Detect, Respond, and Recover—organized into 23 categories as illustrated by the figure below. This structure, as it has been used within the Luxembourg

[15] Market Radar, Source: ECSO, Last Accessed: 15/11/2023, Link: https://ecs-org.eu/activities/market-radar/

[16] Cybersecurity Framework Components, Source: NIST, Last Accessed: 15/11/2023, Link: https://www.nist.gov/cyberframework/online-learning/cybersecurity-framework-components

cybersecurity ecosystem, helps to understand market trends, identify gaps and opportunities, and provides a list of players capable of assisting organizations in strengthening their security. It also offers a clear, non-technical framework to facilitate communication.

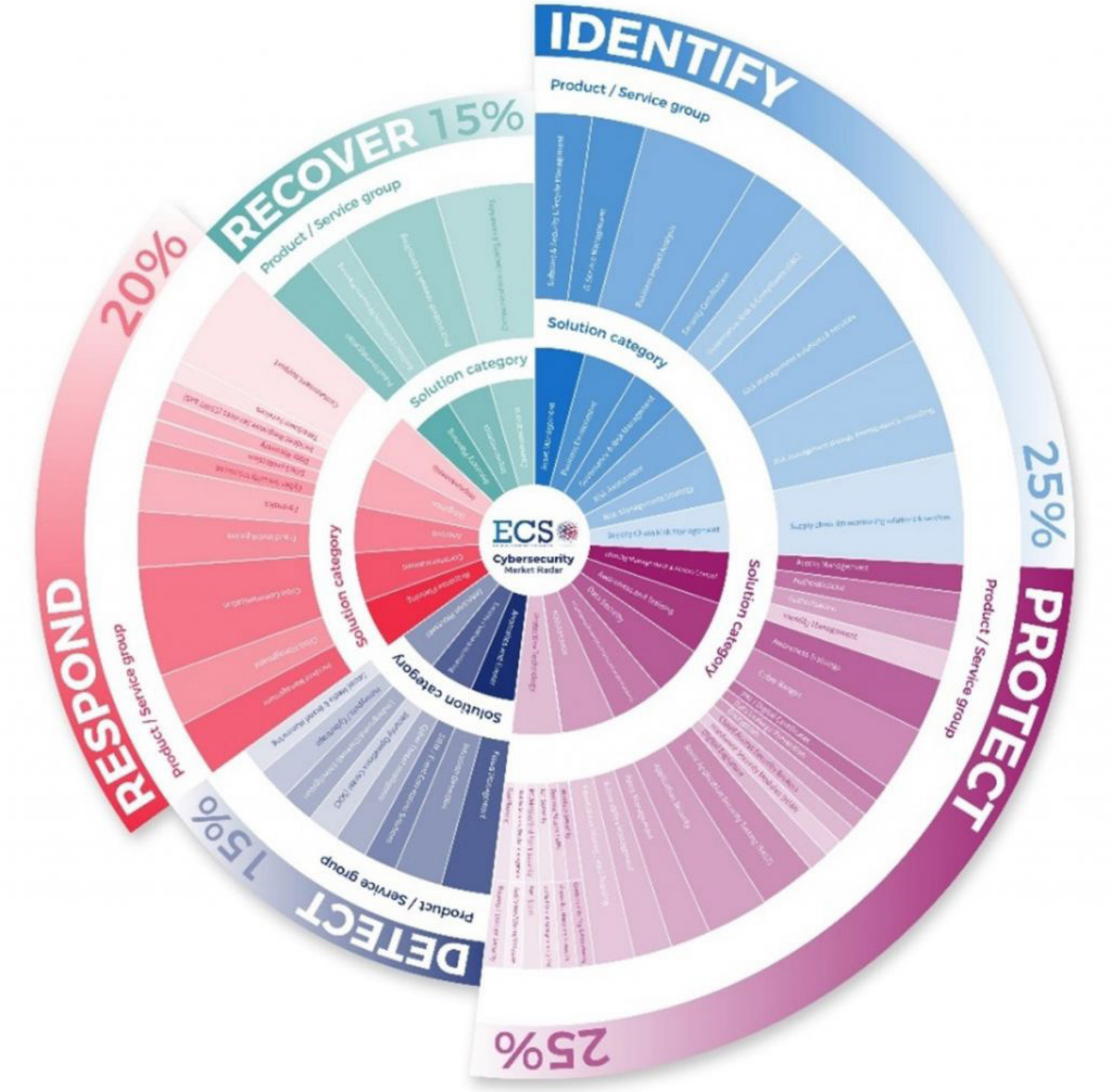


Figure 7: Data sources used by LXI-Market Intelligence for mapping market players

1.6 – An ongoing discussion with market players

The identification and categorization of private companies constituting the national cybersecurity ecosystem were the initial steps toward an ongoing relationship between them and the consortium members who manage the CYBERSECURITY Luxembourg platform. This platform functions as a registry, a promotional tool, and a method for members to register and update their information, thereby keeping the dataset current. Additionally, utilizing the ECSO market radar's classification has enabled comparisons and collaborations with other ecosystems, particularly in cybersecurity. This includes the development of ECSO-led activities such as the Cybersecurity Smart Regions,[17] paving the way for more ambitious projects driven by the European Commission, like the European Cybersecurity Competence Centre (ECCC).[18]

Within this framework, the Luxembourg House of Cybersecurity's NC3 department has been designated as the national coordination center, undertaking new missions of directing market research to provide insights for local players and European partners. This mission aligns with the expanded competencies of the European Union Agency for Cybersecurity (ENISA), as granted by the Cybersecurity Act.[19] It is structured within the Cybersecurity Market Analysis Framework (ECSMAF),[20] which also employs the ECSO market taxonomy. Employing shared research methodologies, taxonomies, and tools can streamline and enhance collaboration, thereby elevating the quality of insights and understanding of market gaps and needs both collectively and individually among EU member states. An example of research methodologies available within the ECSMAF, which was utilized by the market intelligence team of the LHC / NC3 to structure its work and generate comparable metrics on the national ecosystem, is displayed below.

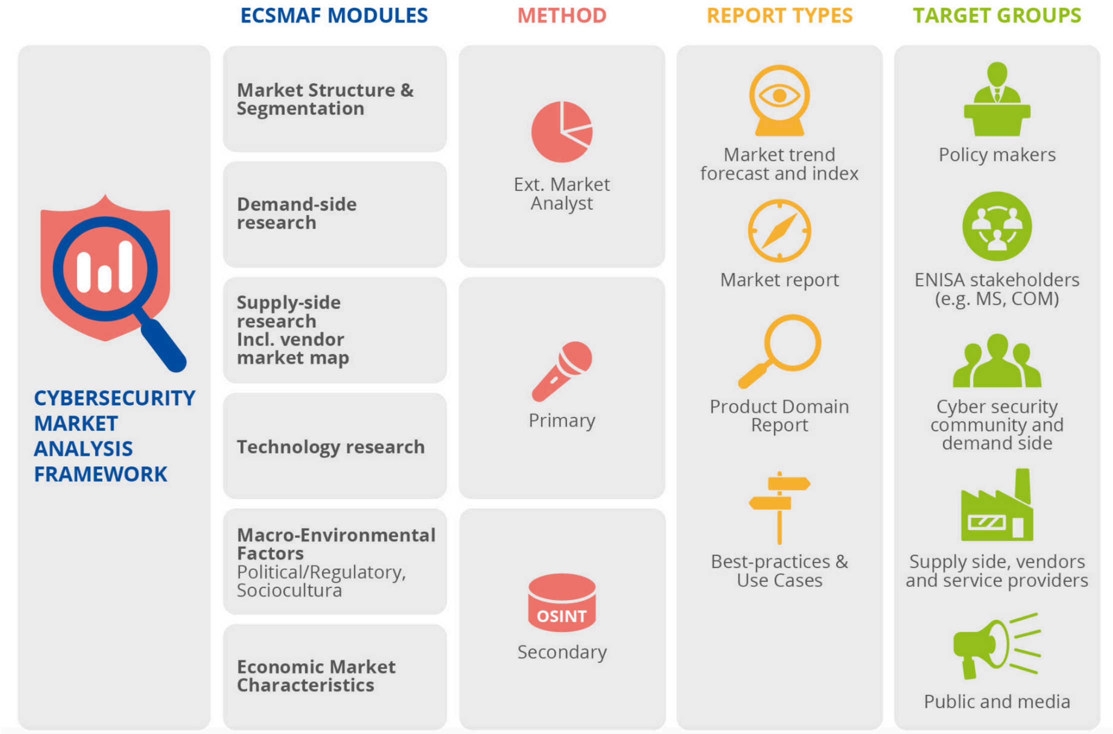

ECSMAF MODULES
METHOD
REPORT TYPES
TARGET GROUPS
CYBERSECURITY MARKET ANALYSIS FRAMEWORK
Market Structure & Segmentation
Demand-side research
Supply-side research Incl. vendor market map
Technology research
Macro-Environmental Factors Political/Regulatory, Sociocultura
Economic Market Characteristics
Ext. Market Analyst
Primary
OSINT
Secondary
Market trend forecast and index
Market report
Product Domain Report
Best-practices & Use Cases
Policy makers
ENISA stakeholders (e.g. MS, COM)
Cyber security community and demand side
Supply side, vendors and service providers
Public and media

Figure 8: Logical blocks/modules of ECSMAF

[17] Smart Specialisation Platform – Cybersecurity, Last Accessed: 15/11/2023, Link: https://s3platform.jrc.ec.europa.eu/cybersecurity

[18] European Cybersecurity Competence Centre (ECCC) and Network, Source: ECCC, Last Accessed: 15/11/2023, Link: https://cybersecurity-centre.europa.eu/about-us_en

[19] Cybersecurity market analysis is a topic that plays an important role in regulation (Cybersecurity Act (CSA), Source: ENISA, Last Accessed: 15/11/2023, Link: https://www.enisa.europa.eu/topics/market

[20] ENISA Cybersecurity Market Analysis Framework (ECSMAF), Source: ENISA, Last Accessed: 15/11/2023, Link: https://www.enisa.europa.eu/publications/enisa-cybersecurity-market-analysis-framework-ecsmaf

1.7 - Sneak peak into CYBERSECURITY Luxembourg ecosystem

The cybersecurity market in Luxembourg is characterized by a high level of competition, with a large number of vendors offering a wide range of solutions. The CYBERSECURITY Luxembourg platform provides insightful data on the local market, indicating a dynamic ecosystem with a total of 311 companies, including 26 established in the last five years and 70 startups. While this number may seem significant, it should be put into perspective considering the overall number of companies, which amounts to around 41,000 entities based on STATEC figures from 2023.[21] In this context, cybersecurity players represent only approximately 0.76% of the total. Of these cybersecurity companies, 85 entities focus primarily on cybersecurity, representing the core of their business. This focus is even more pronounced among startups, with 41% of the 70 start-ups dedicated to cybersecurity as their main activity. The market is diverse in its service and product offerings, categorized under five main groups: PROTECT (204 companies), IDENTIFY (176 companies), RESPOND (74 companies), DETECT (68 companies), and RECOVER (38 companies). Notably, only 12 companies offer comprehensive solutions across all these service/product groups, showcasing a specialized market with focused expertise in various cybersecurity domains. 10 companies are classified as 'PC doctors,' specializing in supporting individuals facing incidents. In terms of public entities, such as ministries, public agencies, and regulators, there are 40 significant players, along with 13 clubs, associations, and initiatives representing cybersecurity experts and organizations contributing to the ecosystem.

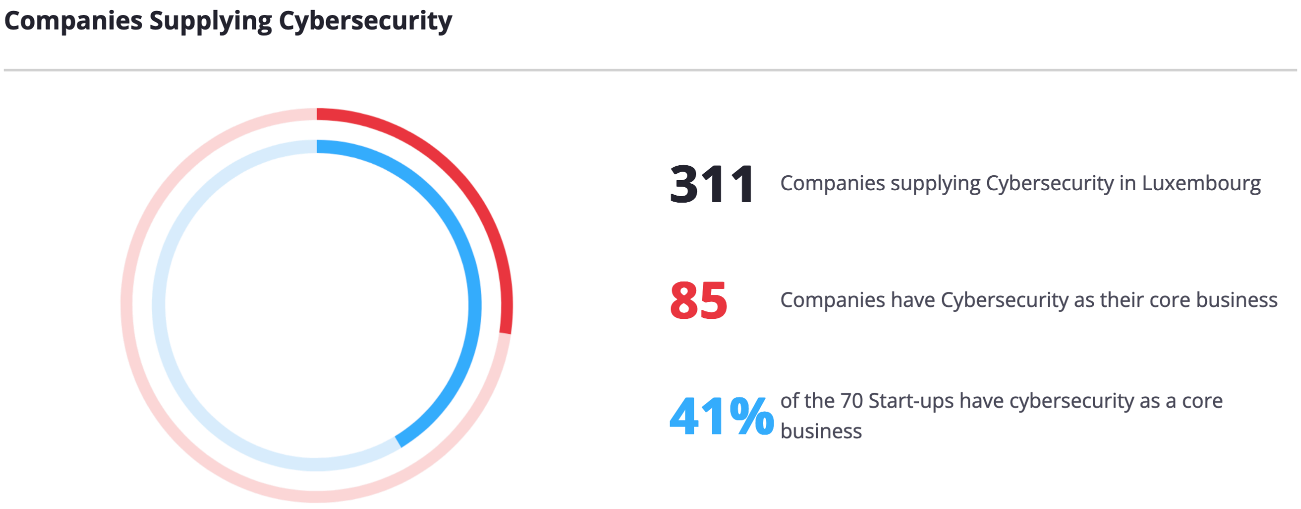


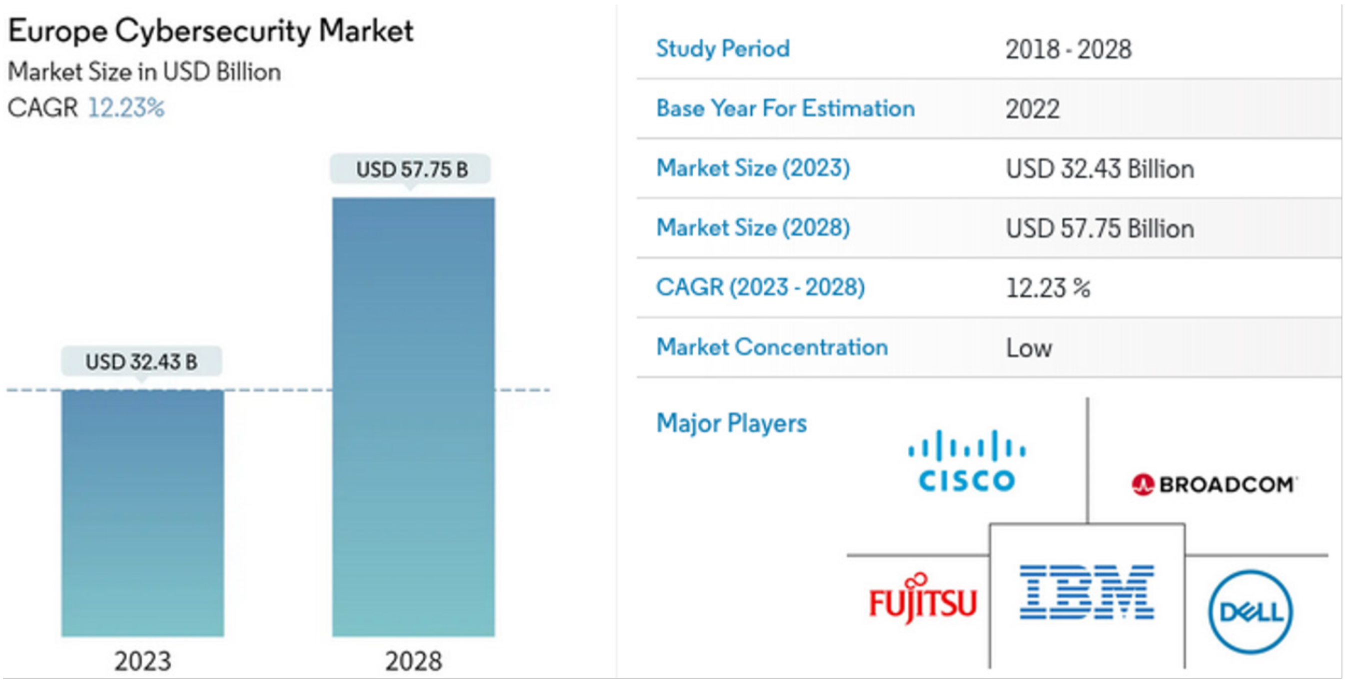
Figure 9: Luxembourg cybersecurity ecosystem private sectors key figures as of November 21, 2023

[21] Statistical portrait of Luxembourg's businesses Edition 2023, Source: STATEC, Last Accessed: 23/01/2024, Link: https://statistiques.public.lu/en/publications/series/analyses/2023/analyses-02-23.html

2 – Financial insights about the market size and forecast

2.1 – European cybersecurity market dynamics and forecast

The European cybersecurity market, according to both Mordor Intelligence[22] and Statista,[23] is poised for significant growth in the coming years, though their projections vary slightly. Statista projects the market's revenue to hit US$40.73 billion in 2023, a significant figure that underlines the sector's rapid expansion. This growth trajectory is set to continue, with Mordor Intelligence forecasting the market to grow from USD 32.43 billion in 2023 to USD 57.75 billion by 2028, at a compound annual growth rate (CAGR) of 12.23%, and Statista estimating it reaching US$66.38 billion by 2028 with a CAGR of 10.26%. Both sources agree on the upward trend and highlight key factors fueling this growth, such as the increasing demand for digitalization, the expansion of the Internet of Things (IoT), and the growing need for cybersecurity solutions in the wake of rising cyber threats and the implementation of EU legislation. Mordor Intelligence emphasizes the impact of COVID-19 in amplifying the need for digital security, while Statista points out the significant contribution of the Security Services segment, expected to generate US$22.22 billion in 2023.



Study Period	2018 - 2028
Base Year For Estimation	2022
Market Size (2023)	USD 32.43 Billion
Market Size (2028)	USD 57.75 Billion
CAGR (2023 - 2028)	12.23 %
Market Concentration	Low
Major Players	CISCO BROADCOM FUJITSU IBM DELL

Figure 10: Key figures of the European cybersecurity market by Mordor Intelligence, with major players listed in no particular order

[22] Europe Cyber Security Market Size & Share Analysis – Growth Trends & Forecasts (2023 – 2028), Source: Mordor Intelligence, Last Accessed: 16/11/2023, Link: https://www.mordorintelligence.com/industry-reports/europe-cybersecurity-market

[23] Cybersecurity – Europe, Source: Statista, Last Accessed: 16/11/2023, Link: https://www.statista.com/outlook/tmo/cybersecurity/europe

Additionally, both sources note the competitive nature of the market, dominated by global players, and the strategic moves such as partnerships and product launches that are shaping the industry's landscape in Europe. The dominance US-based players is attributed to their benefit from a highly innovative domestic market and substantial revenues. In 2023, the United States is expected to lead in revenue generation globally, with an anticipated US$71 billions, as per Statista's analysis. This highlights the significant role of American companies such as IBM, CISCO, and DELL in shaping cybersecurity trends and innovations, not just domestically but also in influencing the European market. This transatlantic influence is a key factor in understanding the dynamics and competitive nature of the European cybersecurity market.

2.2 – Challenges in assessing Luxembourg's cybersecurity market landscape

Uncovering detailed figures that accurately capture the complexity of Luxembourg's cybersecurity market poses a challenge. This difficulty arises from several factors: the dominance of foreign companies that integrate their local operations into broader BENELUX activities, a diverse range of market players, the lack of public financial reporting by these entities, and a general scarcity of data due to a limited number of studies focusing on the country. These challenges are not exclusive to Luxembourg, as underscored in the European Investment Bank's report on cybersecurity investment.[24] The market assessment reveals that data on cybersecurity investments are scarce, making it challenging to develop a comprehensive market overview. Cybersecurity spending often merges with general IT spending, making it difficult to distinguish. For example, most national audit offices lack a centralized view of cybersecurity-related public spending, and no EU Member State mandates separate reporting of cybersecurity expenses in financial plans. The European Investment Bank (EIB) attempted to estimate cybersecurity investments in European Security Initiative (ESI) projects, but this estimation faced assumptions and limitations.

2.3 –Financial analysis of the Luxembourg cybersecurity ecosystem pure players

As a basic approach to generating market figures for the national landscape, we explored the available data of cybersecurity pure players, companies that specialize exclusively in cybersecurity-related products or services, listed in the Luxembourg cybersecurity ecosystem register.[25] The foundational data for this financial analysis of Luxembourg's cybersecurity market were drawn from public records of annual accounts (eCDF), specifically for the fiscal years spanning from January 1, 2021, to December 31, 2021, and January 1, 2022, to December 31,

[24] European Cybersecurity Investment Platform, Source: European Investment Bank, Last Accessed: 15/11/2023, Link: https://www.eib.org/en/publications/20220206-european-cybersecurity-investment-platform

[25] Private sector entities – category core business, Source: CYBERSECURITY Luxembourg, Last Accessed: 21/11/2023, Source: https://www.cybersecurity.lu/ecosystem?corebusiness_only=true&

2022. accessible from the Trade and Companies Register (RCS) of the Luxembourg Business Registers[26] (LBR). The LBR is an economic interest grouping formed by the State, the Chamber of Commerce, and the Chamber of Crafts of the Grand Duchy of Luxembourg. Our focus was primarily on the sections detailing "Profit or Loss for the Financial Year," as well as capital, reserves, and liabilities. In addition to financial data, our study also included an examination of the employee counts within these companies based on the same sources.

- Dataset includes 84 companies which are listed as cybersecurity pure players in the Luxembourg cybersecurity ecosystem register.
- Financial statements are not available for 11 companies since at least 2021.
- 2022 financial information is unavailable for 13 companies, but data from 2021 are available.

The employee data, represented in full-time equivalent (FTE) rather than absolute numbers, is limited to the companies in the Luxembourg cybersecurity ecosystem register. This approach does not account for potentially larger workforces in subsidiaries or parent companies, thereby affecting the perception of the market's workforce size. Additionally, the operational and financial structures of some companies are complex, with subdivisions into multiple entities for compliance with specific rules like Support PSF (Professional of the Financial Sector), which can result in variations in employee numbers and revenues. Despite the lack of key information, such as detailed sales figures in the documents, the following results constitute an attempt to compile partial public data to offer some insights into the market.

Employee Data Overview (2022 and 2021)

- Employee figures were available for 59% of the total dataset (49 companies), based on information from 2022 or, for some companies, 2021 when the former was unavailable
- The average number of employees per company was 19, with a median of 3, indicating a significant concentration of smaller-sized entities in this sector.
- The total employee count summed up to 932.38, with a notable majority (61%) of companies employing fewer than 5 people.

Financial Year 2022 Performance

- Financial details were available for 71% of the dataset (60 companies).
- There was a substantial average profit of €7,5 millions (M) compared to a median of 0.012M, highlighting significant financial disparities among companies.
- The total profit or loss amounted to approximately €449.5 million.
- A closer look at the data reveals that 32% of these companies incurred losses, averaging

[26] Trade and Companies Register (RCS), Source: Luxembourg Business Registers, Last Accessed: 21/11/2023, Source: https://www.lbr.lu/mjrcs

-€0.6M, while the remaining 68% achieved profits, averaging €11.2M.

Financial Year 2021 Performance

- Coverage extended to 86% of the dataset (72 companies).
- The average profit or loss was considerably lower at €0.006M, with a median of €0.023M, reflecting a potentially more evenly distributed financial landscape in this period.
- The total profit or loss for 2021 stood at about €0.46M.
- The distribution between loss-making and profit-making companies remained consistent with 2022, with 32% recording losses (average of -€0.5M) and 68% making profits (average of €0.25M).

Capital, Reserves, and Liabilities

- For 2022, data from 60 companies (71% of total) showed an average capital, reserves, and liabilities figure of over €12M and a median of around €0.4M, amounting to a total of over €712M.
- In comparison, the 2021 data for 73 companies (87% of total) revealed lower averages and totals – an average of approximately €4.3M and a total of over €314M, with a median value around €0.3M.

3 – Results from our survey

3.1 - Capturing data from Luxembourg's cybersecurity market

In addition to analyzing the national ecosystem figures and financial data of core cybersecurity entities within the ecosystem, we considered collecting more information from market players through an additional source. This part of our research was designed to generate quantifiable data, allowing us to pinpoint specific market trends and provide essential insights into the challenges faced by stakeholders. We developed the questions of our survey in collaboration with cybersecurity professionals, experts and business owners, from various companies, supported by the Chamber of Commerce economist team. This survey, distributed online from September 29 to November 27, was designed to capture a broad range of perspectives. Given Luxembourg's status as a smaller market with limited existing studies and open data about its players, this survey was particularly crucial in supporting the development of the cybersecurity ecosystem by generating insights and figures about the market.

We have the following breakdown of the survey responses according to their completion status:

- Total number of survey participants: 64 (100%)
- Number of completed surveys 22 (34.4%)
- Number of unfinished surveys: 42 (65.6%)

Based on the number of companies listed as providing cybersecurity services, this survey potentially represents approximately 7% of the total number of companies that make up the CYBERSECURITY Luxembourg ecosystem.[27]

The dataset of answers is organized into several categories as shown below, with each section including only the fully completed responses (22 in total), as per the structure used in the online survey. It began by gathering socio-economic details of the SMEs to categorize the participants.

3.2 - Socio-economic data

In the preliminary section of our market intelligence report on Luxembourg's cybersecurity providers, we analyze socio-economic data to better understand the profiles of the respondents. Regarding company size, the data reveals a notable presence of both large and very small companies within the industry. Specifically, the survey shows that 7 of the responding companies have 250 or more employees, suggesting the existence of substantial players in this sector. On the other end of the spectrum, 4 companies have 5 employees or fewer, indicating a segment of

[27] Private sector entities – category core business, Source: CYBERSECURITY Luxembourg, Last Accessed: 30/11/2023, Source: https://cybersecurity.lu/ecosystem

the market occupied by small-scale operations or startups.

When addressing the challenges in human resources, specifically in terms of finding, hiring, and retaining cybersecurity professionals, a majority of respondents (18 out of 22) acknowledge this as a significant hurdle. This finding highlights a critical challenge faced by the industry in securing skilled talent, which is essential for operational growth and sustainability.

Q1 – How many employees does your business have?

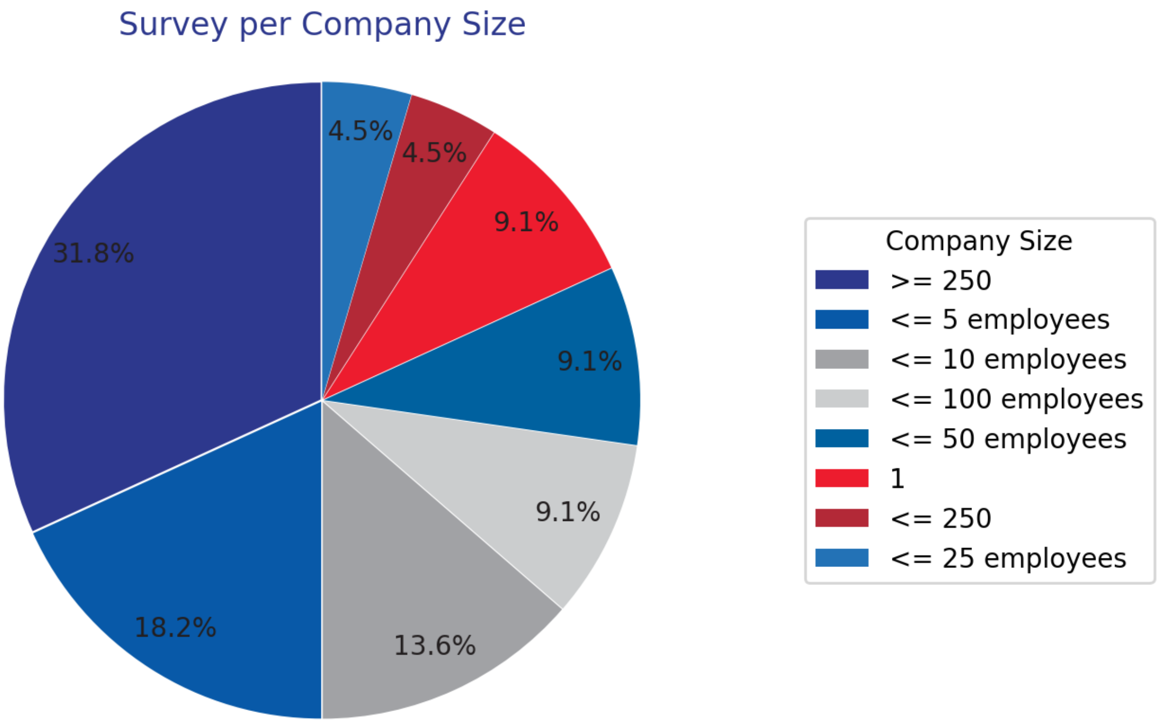


Figure 11: Distribution of answers to the NC3 cybersecurity providers survey by employee count

Q2 – Are human resources challenges a significant hurdle for you in terms of finding, hiring, and retaining cybersecurity professionals?

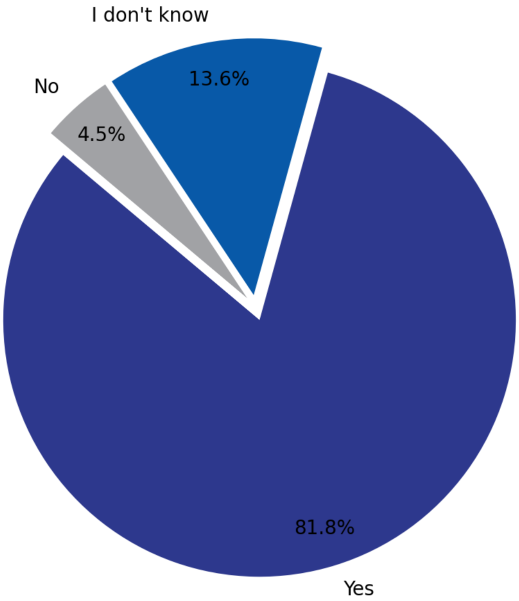


Figure 12: Human resources challenges in finding, hiring, and retaining cybersecurity professionals – responses from the NC3 cybersecurity providers survey

3.3 - SME and cybersecurity

In the segment focusing on SMEs and cybersecurity, we examine the perspectives of Luxembourg's cybersecurity providers regarding their interactions and services for SMEs. This analysis provides insights that can further inform the findings from our previous study on the cybersecurity challenges and opportunities in Luxembourg's SME sector[28] regarding the availability of services for this type of entities and their level of maturity in information security.

Concerning dedicated cybersecurity offerings for SMEs, the responses are varied, indicating a diverse approach within the industry. Notably, 6 respondents state they have a solution specifically for SMEs, while another 6 offer different services for small and medium-sized companies, suggesting a tailored approach to this market segment. However, 7 respondents do not focus on SMEs, and 3 provide general services for all types of companies, reflecting a broader market strategy that does not differentiate by company size.

When interacting with SMEs on cybersecurity threats and solutions, the responses highlight a range of engagement levels and understanding among SMEs. Four respondents note that SMEs understand cybersecurity concerns if they have an in-house IT expert, whereas two respondents find understanding if the SME has experienced an incident. This suggests that SMEs' understanding of cybersecurity is often linked to their prior exposure or internal expertise, indicating that risk perception is still very much tied to specific technical skills and/or real, direct experience.

[28] A Comprehensive Market Study on Cybersecurity Challenges and Opportunities in Luxembourg's SME sector, Source: NC3 Cybersecurity Observatory Last Accessed: 30/11/2023, Source: https://observatory.nc3.lu/market-intelligence-library/report-2023/

Regarding the factors that encourage SMEs to invest in cybersecurity, the most frequently cited reasons are incident experience and lessons learned (12 responses) and management awareness of cybersecurity topics (11 responses). This highlights the importance of direct experience and top-level awareness in motivating SME investments in cybersecurity.

In assessing the costs and budget allocation for SMEs' cybersecurity investments, the most common methods include compliance and best practices prioritization (7 responses) and risk-based budgeting (6 responses). Notably, 8 respondents do not carry out such assessments, pointing to a potential gap in understanding or addressing the financial aspects of cybersecurity for SMEs.

In the "Other" category, which comprises comments from respondents, the survey uncovers valuable qualitative insights about market perspectives among Luxembourg's cybersecurity providers in their dealings with SMEs. These comments reveal diverse and tailored strategies: a collaborative approach where cybersecurity is woven into a broader IT service framework, specifically catered to the unique needs and financial capabilities of SMEs; a holistic strategy that integrates cybersecurity within the overall risk and governance structure of an organization, indicating a perspective that views cybersecurity as an integral component of business governance; and a risk-centric approach, where discussions with SMEs begin by assessing their specific exposure to cyber risks and the potential business repercussions, suggesting a focus on tailored, risk-aware strategies in managing cybersecurity for SMEs. These insights reflect the depth and variety in the approaches taken by cybersecurity providers to address the distinct needs of SMEs in the cybersecurity landscape.

Q3 – Does your company have a dedicated cybersecurity offering for SMEs?

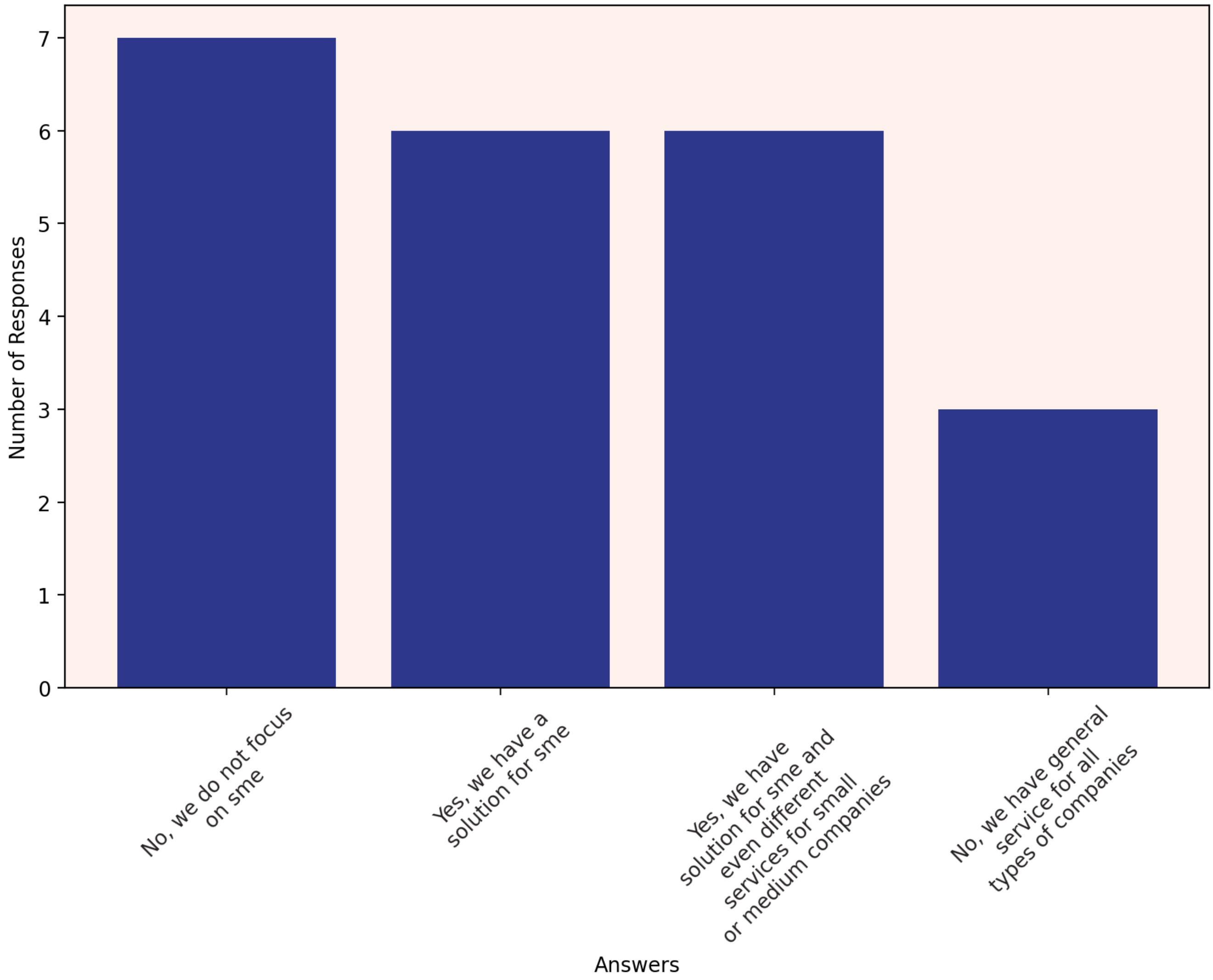


Figure 13: Availability of dedicated cybersecurity solutions for SMEs – responses from NC3 cybersecurity providers survey

Q4 – In your interactions with SMEs, do you specifically address the subject of cybersecurity threats and solutions?

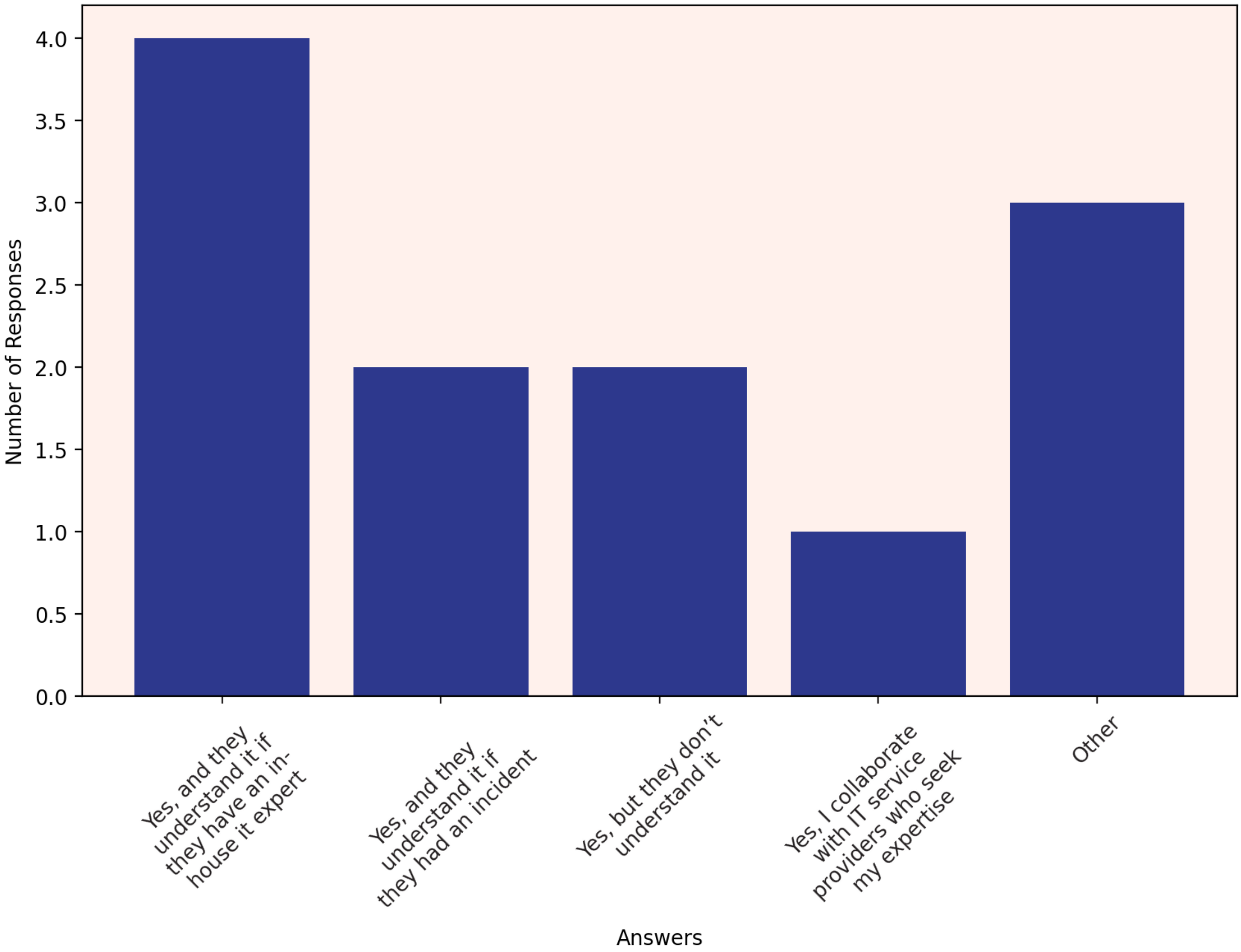


Figure 14: Distribution of responses on addressing cybersecurity with SMEs in the NC3 cybersecurity providers survey

The comments shared by respondents in the 'other' category of the survey, which focuses on cybersecurity providers' interactions with SMEs, reveal several key insights:

- Collaborative Approach: One respondent highlights a collaborative approach, working with both IT service providers and SMEs. This implies a strategy where cybersecurity is addressed as part of a broader IT service, tailored to the SME's needs and budget constraints.
- Integrated Security and Governance: Another response emphasizes the integration of cybersecurity with general risk and governance (GRC). This suggests a perspective that sees cybersecurity as inseparable from the overall governance and risk management framework of a company, rather than as a standalone issue.
- Risk-Centric Conversations: The third response indicates an initial focus on discussing

the SME's exposure to cyber risks and the potential implications for their business. This approach suggests a more consultative and risk-aware strategy, starting conversations around the specific cyber threats relevant to the SME's business context.

Q5 – From your market experience, could you outline the factors that encourage SMEs to invest in their cybersecurity?

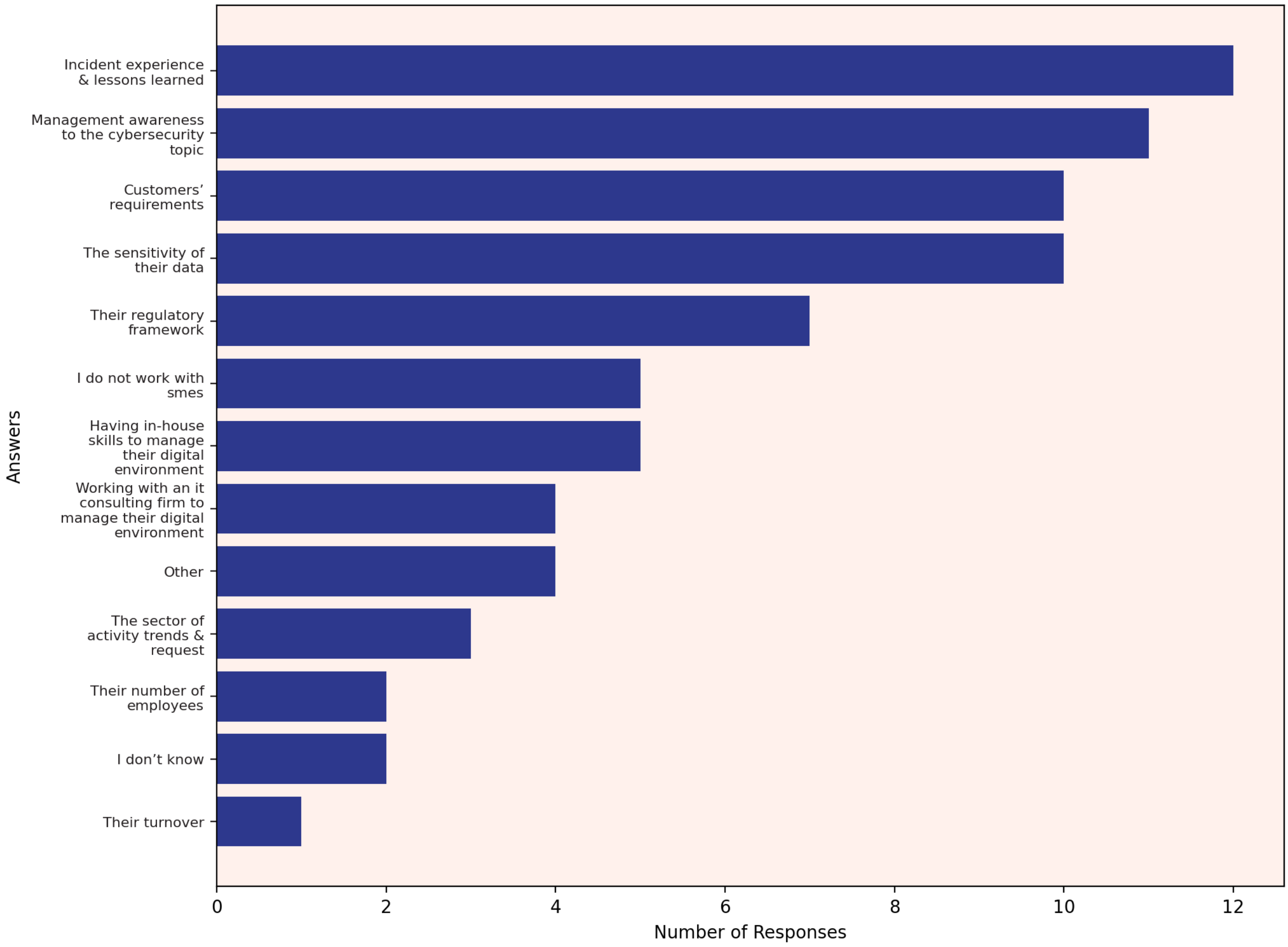


Figure 15: Factors influencing SME investment in cybersecurity – insights from the NC3 cybersecurity providers survey

3.4 - Cost and budget

In examining the cost structure of cybersecurity services offered by Luxembourg providers, the survey responses provide insight into the various pricing models based on service types. When asked about how they generally assess the costs and budget allocated to their SME customers' cybersecurity investments, the providers' responses varied significantly, indicating a diverse range of assessment methods in use.

In terms of the primary drivers for cybersecurity certification investment, the most frequently cited reasons are competitive advantage and employees' skills development, with 15 and 14 mentions respectively. This suggests a strong emphasis within the sector on staying ahead in a competitive landscape and investing in the professional growth of employees.

The results of the survey on cybersecurity cost assessments for SMEs reveals a diverse landscape among Luxembourg providers. Notably, 8 out of 22 do not perform formal assessments, highlighting a gap in structured financial evaluation. Compliance and best practices are prioritized by 7 respondents, and 6 focus on risk-based budgeting, emphasizing regulatory alignment and risk management. Other methods, including risk assessments, operational expenditure (OpEx), and cost-benefit analysis, reflect a balanced approach to operational needs and cost efficiency. Less common strategies involve total cost of ownership (TCO), maturity model-based corrective actions, capital expenditure (CapEx), and incident-triggered remedial costs, with one respondent specifying a unique approach.

When it comes to ad hoc or project-specific cybersecurity services, the pricing appears to be more varied. Three respondents each fall into the higher price brackets of above 1400 euros per day (175 euros per hour) and 1200-1400 euros per day (150-175 euros per hour). This indicates that specialized, project-based services may command a premium price.

For highly specialized expertise or niche tools in cybersecurity, the most quoted price range is again 1000-1200 euros per day (125-150 euros per hour), noted by 5 respondents. This is followed by the above 1400 euros per day bracket, mentioned by 4 respondents. Such pricing reflects the premium value placed on specialized skills and tools in the cybersecurity domain.

Finally, in the case of 24/7 cybersecurity services, a significant number of respondents (9) do not provide such services, indicating a possible gap in the market. Among those who do, the pricing is diverse, with 2 respondents each in the higher price brackets of above 1400 euros per day and 1200-1400 euros per day. This suggests that round-the-clock services are priced at a premium, possibly reflecting the additional resources and commitment required for continuous monitoring and response.

Q6 – What are the primary drivers for cybersecurity certifications investment?

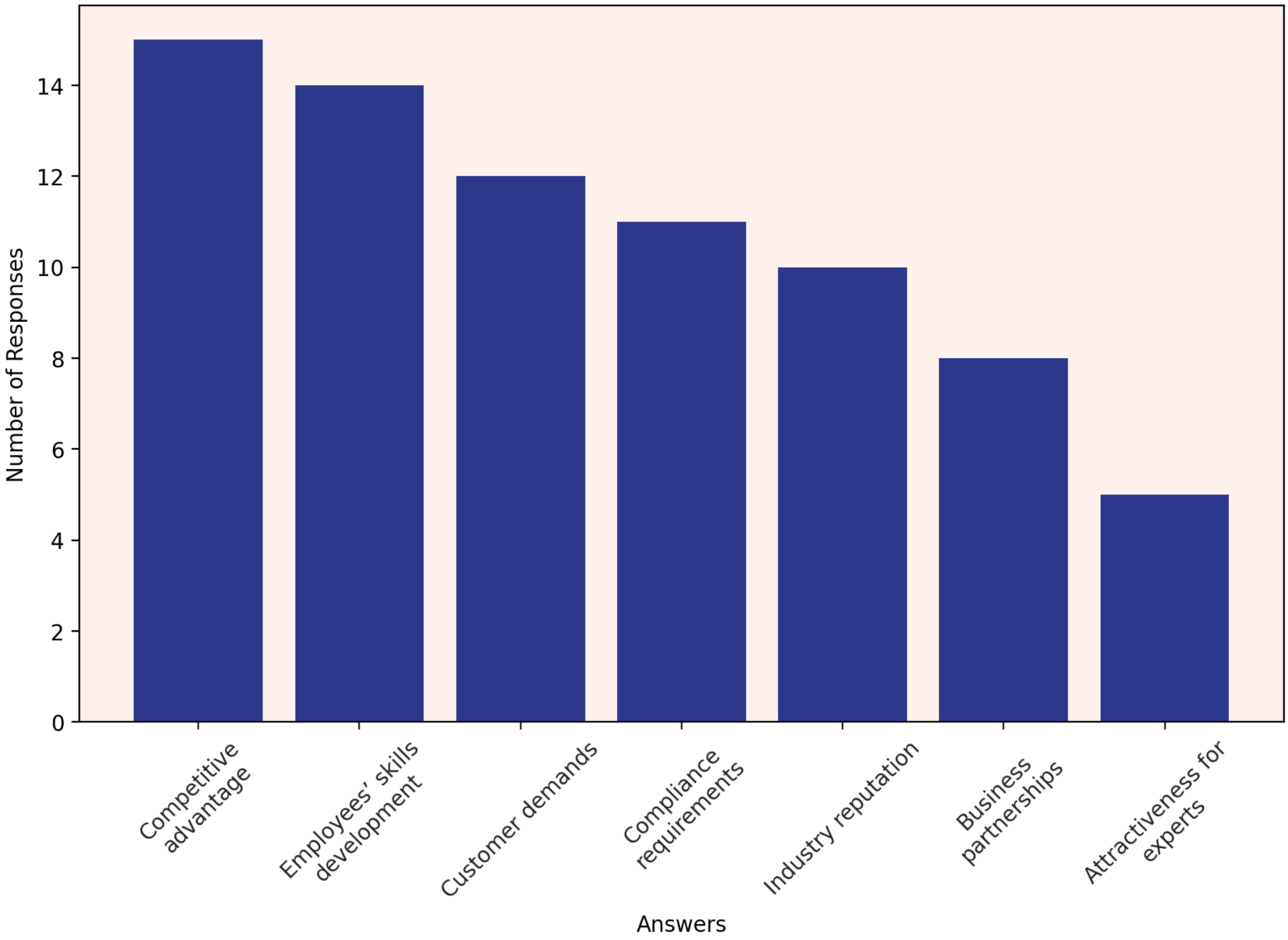


Figure 16: Key motivations for cybersecurity certification investment – NC3 cybersecurity providers survey

Q7 – How do you generally assess the costs and budget allocated to your SME customers' cybersecurity investments?

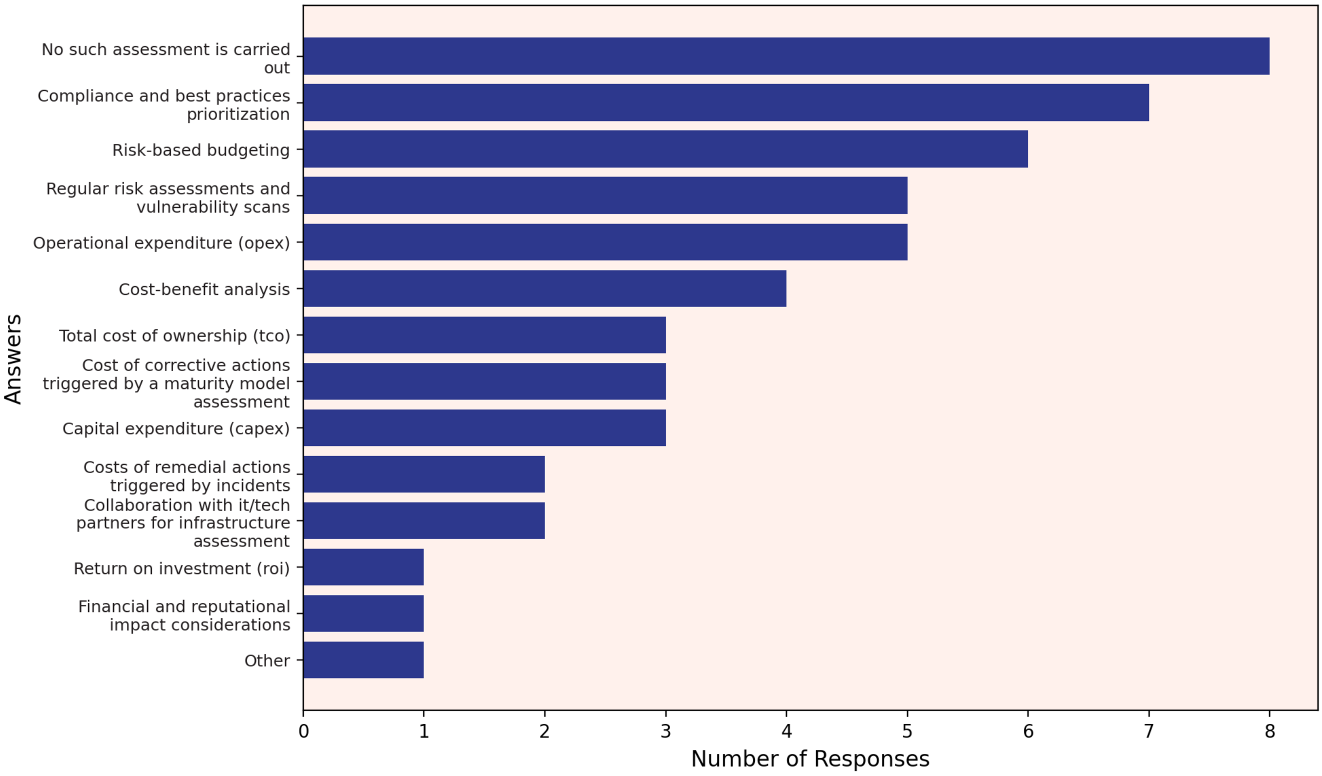


Figure 17: Approaches to assessing cybersecurity investment costs for SMEs – findings from the NC3 cybersecurity providers survey

Q8 – What is the man-day cost paid by customers for your cybersecurity services when provided as part of a comprehensive package?

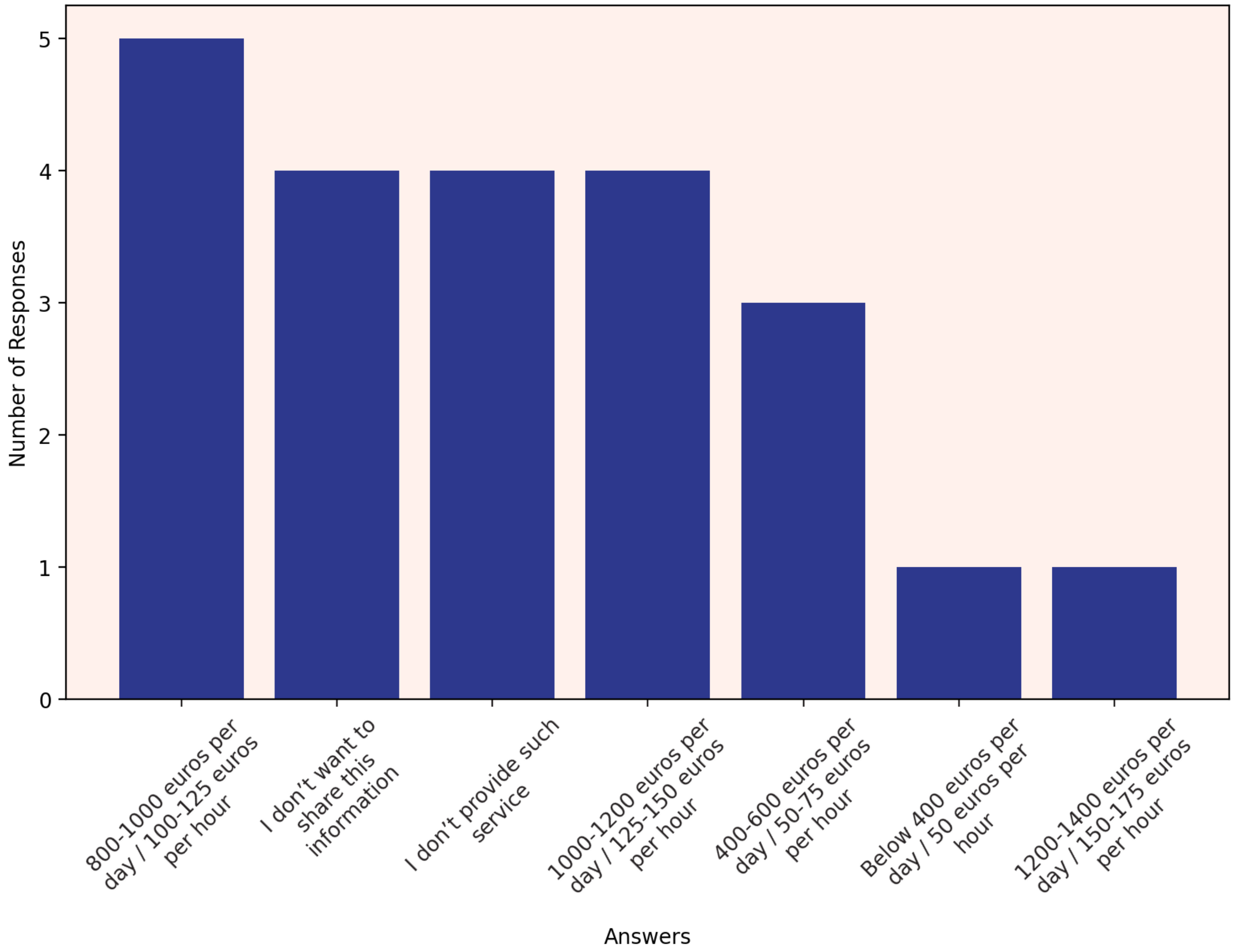


Figure 18: Man-day cost for comprehensive cybersecurity services – insights from the NC3 cybersecurity providers survey

Q9 – What is the man-day cost paid by customers for your cybersecurity services when required on an ad hoc basis or for specific projects?

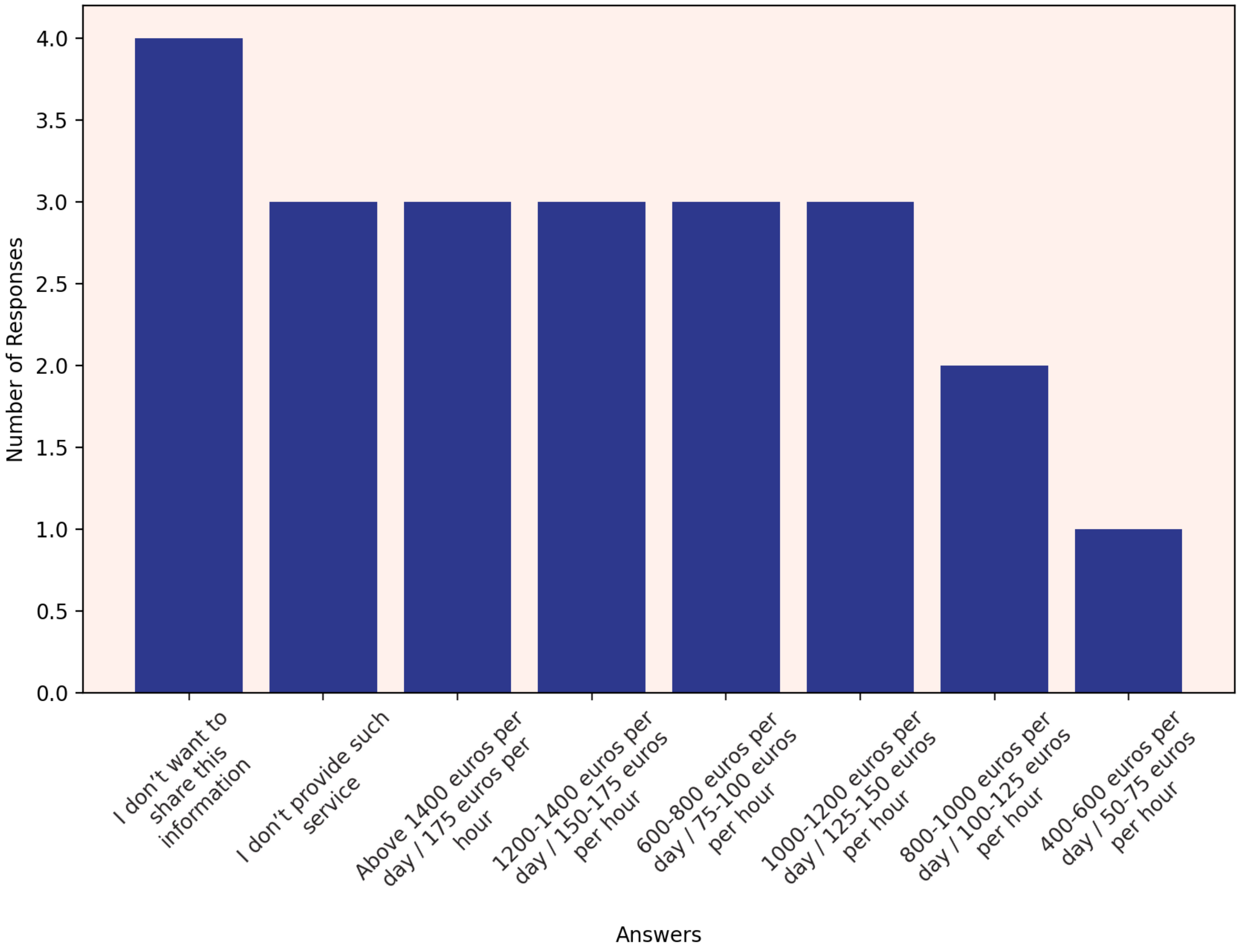


Figure 19: Man-day costs for ad hoc or project-specific cybersecurity services – findings from the NC3 cybersecurity providers survey

Q10 – What is the man-day cost paid by customers for your cybersecurity services for highly specialized expertise or niche tools?

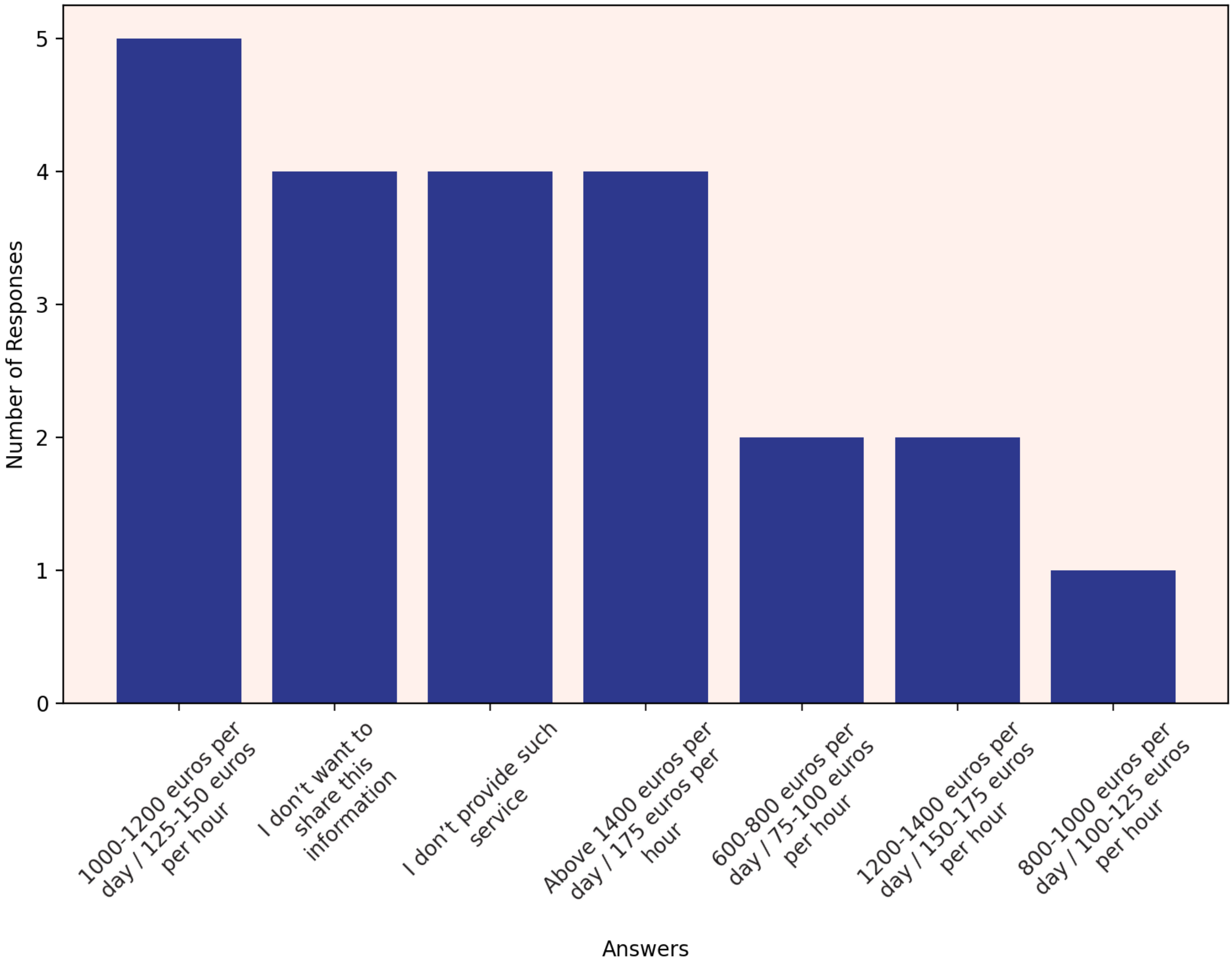


Figure 20: Man-day costs for specialized expertise or niche tools in cybersecurity services – insights from the NC3 cybersecurity providers survey

Q11 – What is the man-day cost paid by customers for your cybersecurity services when offered as a 24/7 service?

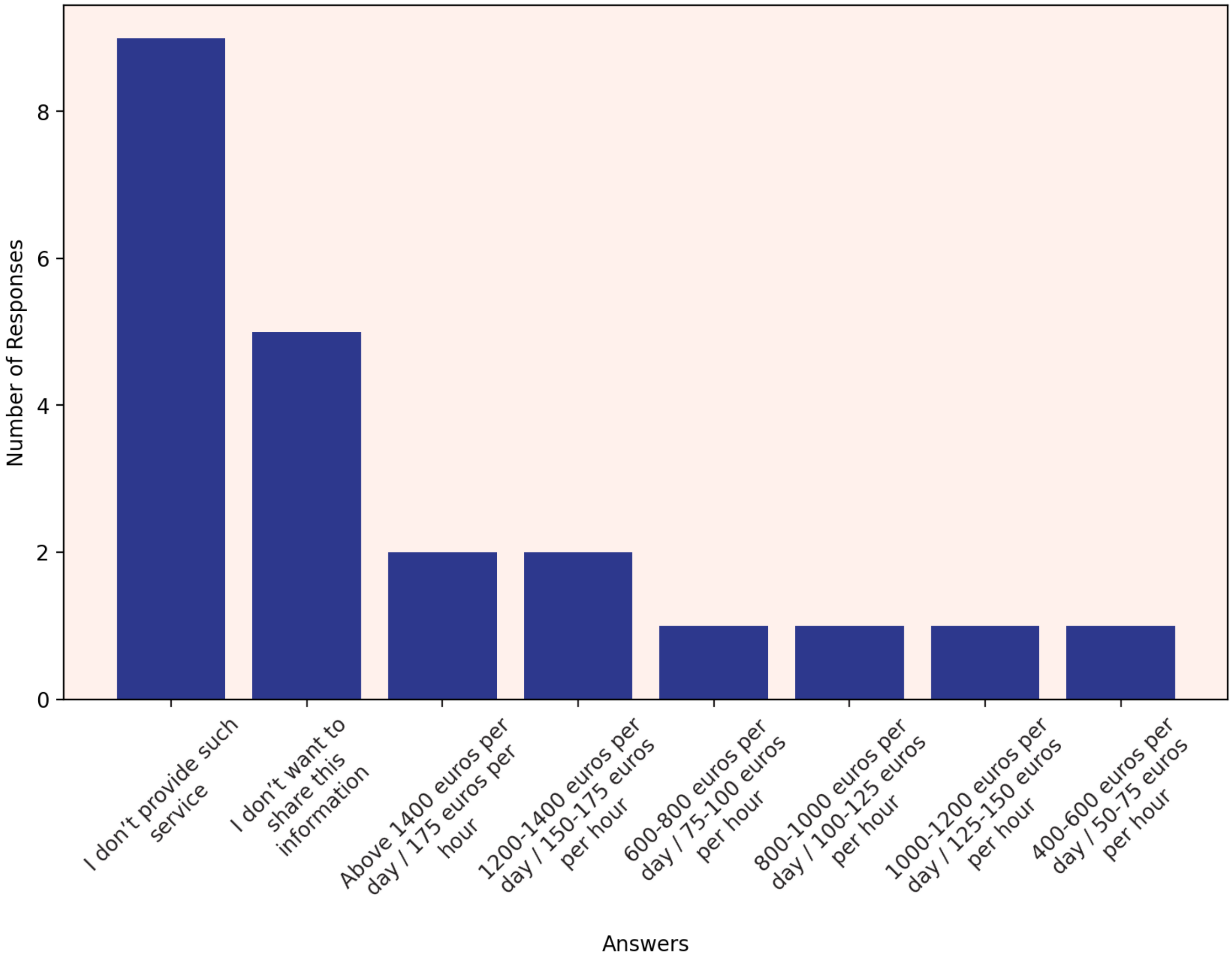


Figure 21: Man-day costs for 24/7 cybersecurity services – findings from the NC3 cybersecurity providers survey

3.5 - Threat trends

In this section of our report on Luxembourg's cybersecurity landscape, we analyze the prevalence of cyberattacks and their impact on businesses in terms of downtime and recovery periods.

The survey indicates a general consensus among cybersecurity providers that cyberattacks targeting companies in Luxembourg have increased. Specifically, 10 respondents observe a sharp rise in the number of attacks, while 9 note a slight increase. This trend underscores the growing challenge of cybersecurity threats in the region.

Regarding the typical duration of complete downtime experienced by a company during a cyberattack, responses vary, reflecting the complexity and severity of such incidents. Four respondents indicate a downtime of 1-2 weeks, while 3 suggest a duration of around 5 days. Lesser durations like less than a day and up to 3 days are also noted, suggesting that the impact of cyberattacks on operational downtime can range significantly.

When asked about the average duration required for a company to recover completely and restore normal operations following a cyber attack, the most common estimate is 1 month, as noted by 7 respondents. This is followed by 3 responses indicating a recovery period of 3 months. The varied responses, which range up to 1-2 years and even include the perspective that a company never fully recovers, highlight the long-term impact and complexity involved in recovering from a cyberattack.

Q12 – Have you observed an increase in the number of cyberattacks targeting companies in Luxembourg over the past few years?

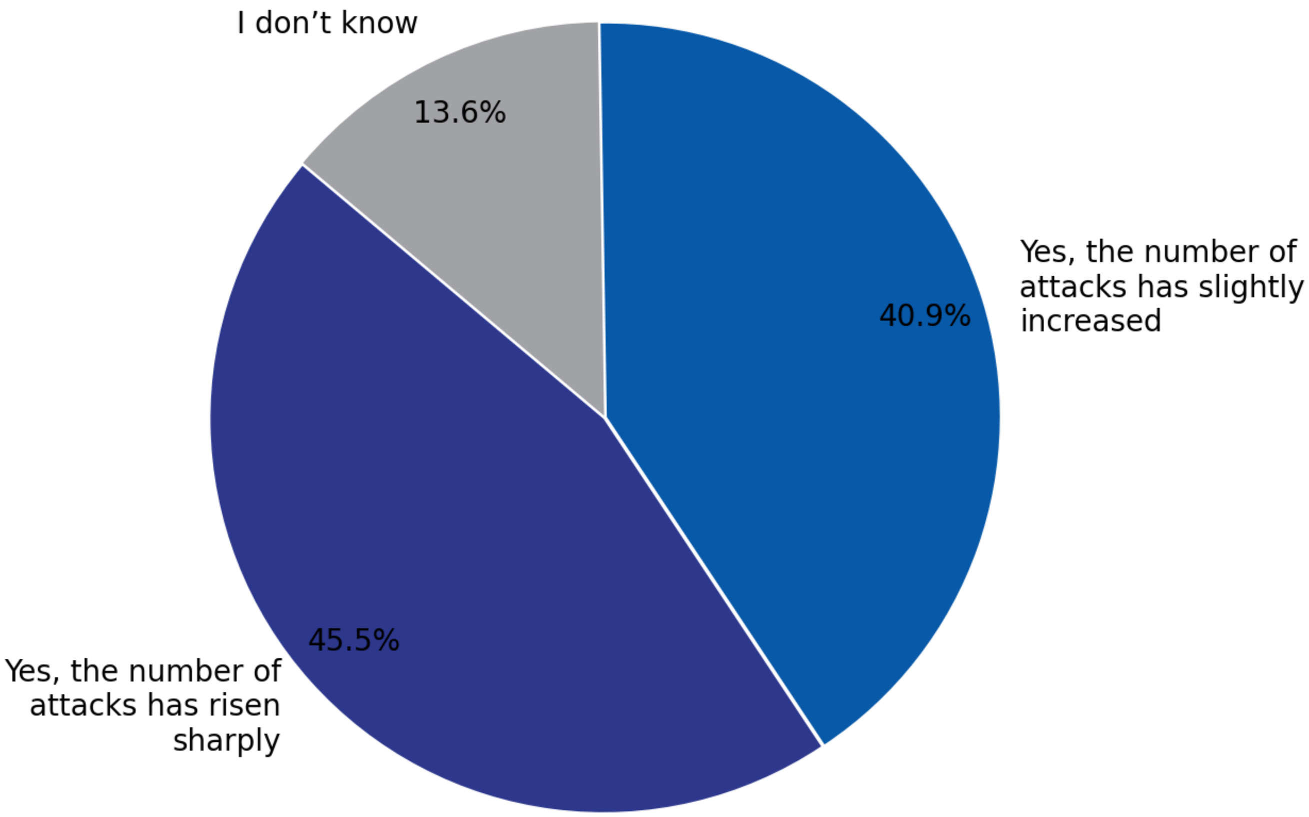


Figure 22: Trends in cyberattacks on Luxembourg companies – responses from the NC3 cybersecurity providers survey

Q13 – What is the typical duration of complete downtime for a company during a cyber attack?

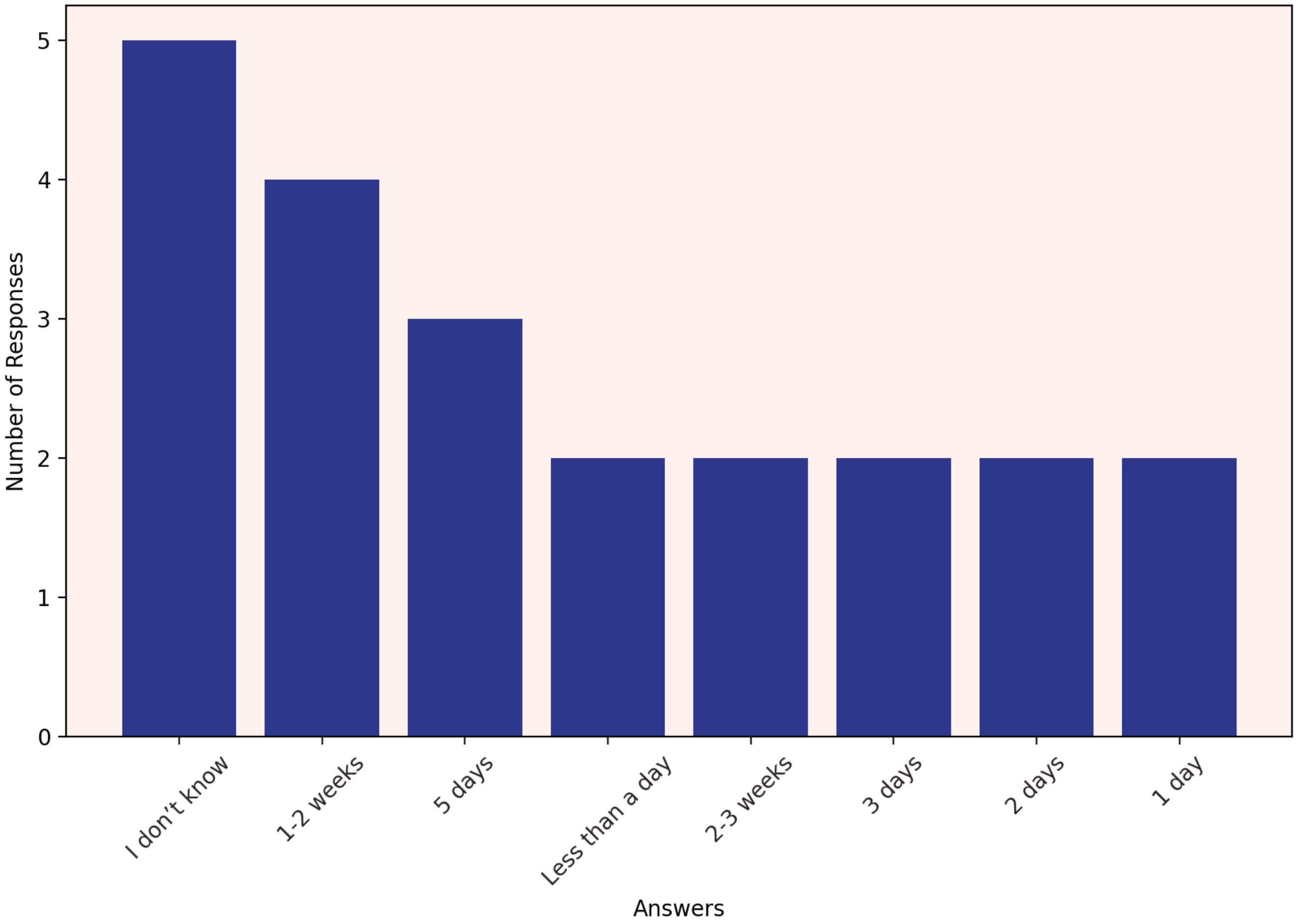


Figure 23: Typical downtime duration during a cyber attack – insights from the NC3 cybersecurity providers survey

Q14 – Can you provide an estimate of the average duration required for a company to recover completely and restore normal operations following a cyber attack?

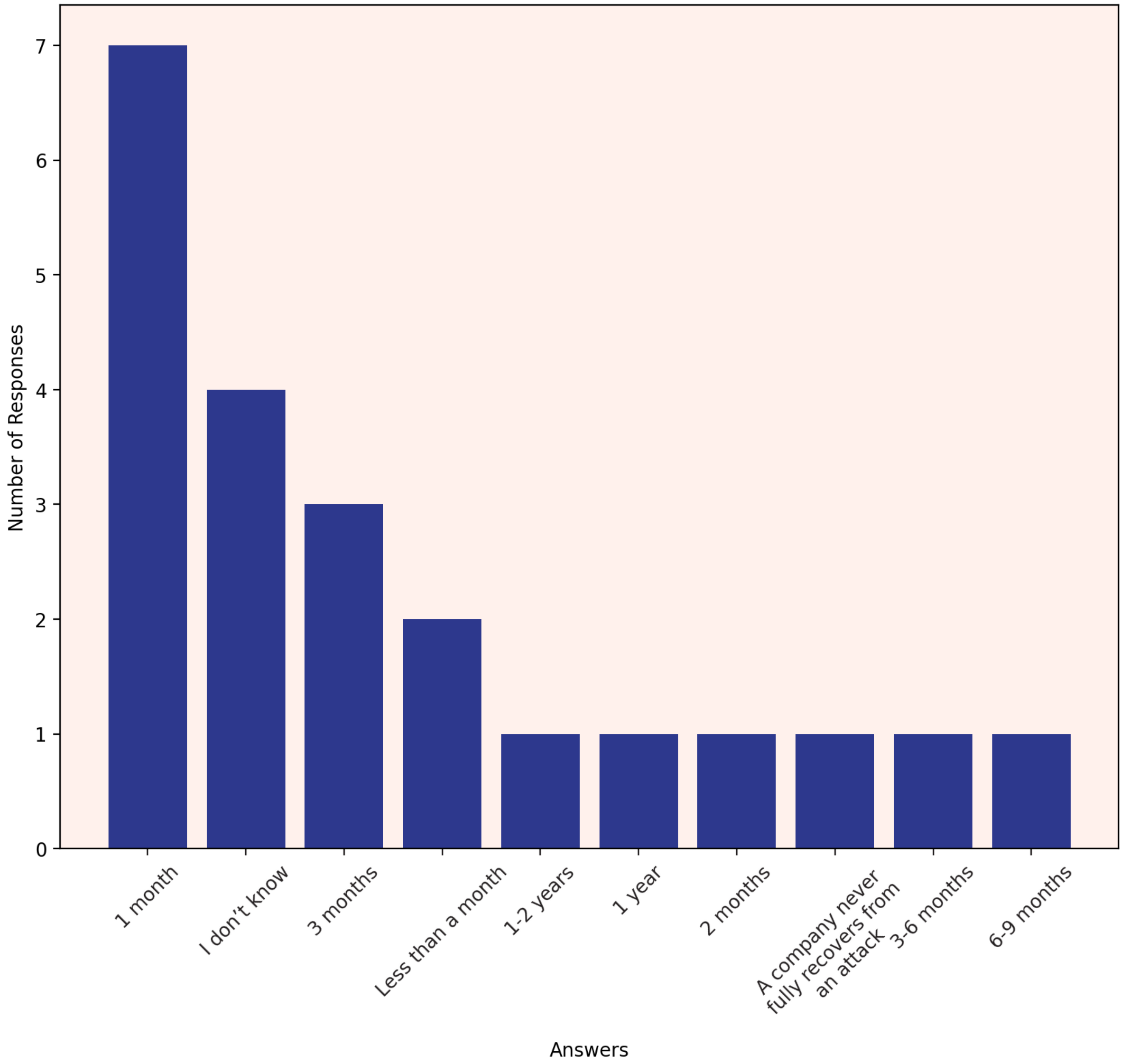


Figure 24: Estimated recovery time post-cyber attack – responses from the NC3 cybersecurity providers survey

3.6 - Market trends

The Luxembourg cybersecurity market is characterized by diverse revenue-generating activities and varied factors influencing solution adoption, along with mixed attitudes towards innovation and open-source solutions. The survey shows consulting and professional services (12 responses), business continuity services (7 responses), and risk assessment and compliance (6 responses) as the top revenue drivers. Additionally, 'Basic Customer Support' and 'Cyber Transformation Program' are identified by individual respondents as crucial for sales, suggesting an emphasis on customer service and comprehensive cybersecurity transformations.

In terms of solution adoption, the complexity for final users (15 responses) and technological trends (12 responses) are prioritized. Technical features, price, and regulation also play a significant role, as per the respondents. One respondent notably prefers Free/Libre and Open Source Software (FLOSS), highlighting a niche focus on customizable solutions.

European origin is a key criterion for 11 respondents in adopting new solutions, indicating a preference for solutions that comply with European standards. However, 6 respondents find the origin irrelevant. The market's openness to innovation is viewed differently, with 9 respondents seeing it as welcoming, while 7 do not, and 6 remain unsure. Challenges to innovation include limited market size and need for continuous trend monitoring, as per individual responses. Concerns about market education, public administration's role in cybersecurity, GDPR gaps, and the centralization of decision-making are also noted.

For integrating open-source solutions, 11 respondents lack a specific approach, whereas 9 have strategies in place. Reasons against integration include customer resistance and concerns in high-risk industries, as indicated by two respondents, one favoring open-source adoption and another from an insurance provider wary of the associated risks. These insights reflect the complexity of the market's approach to open-source solutions, driven by customer preferences and regulatory compliance.

Q15 – What are the top three activities that generate the highest sales for your company within each of the following categories?

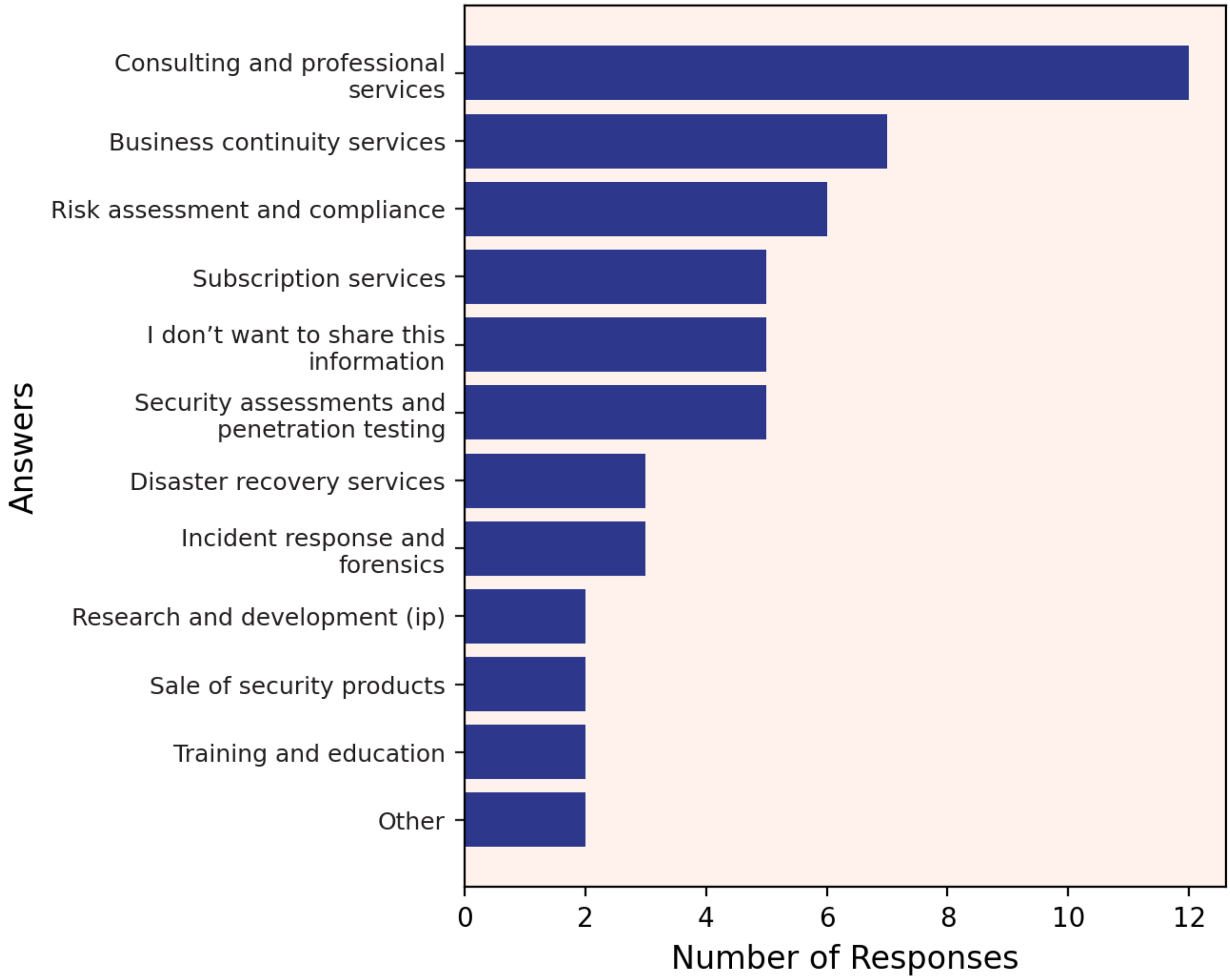


Figure 25: Top revenue-generating activities in cybersecurity – findings from the NC3 cybersecurity providers survey

The comments provided by respondents in the ‘other’ category of the survey, concerning the top three activities that generate the highest sales for companies, reveal specific and specialized areas of focus:

- Basic Customer Support: One respondent identifies ‘Basic Customer Support’ as a significant sales generator for their company. This indicates the importance of customer service in their business model, suggesting that providing reliable and effective support is a key revenue driver. This could encompass a range of activities from troubleshooting to assisting with product usage.
- Cyber Transformation Program: Another response highlights ‘Cyber Transformation Program’ as a key sales-generating activity. This suggests a focus on comprehensive cybersecurity solutions that involve transforming an organization’s digital security pos-

ture. Such programs likely include a suite of services like assessments, strategy development, implementation of security measures, and ongoing support.

Q16 – What factors do you consider when assessing the solutions your business adopts?

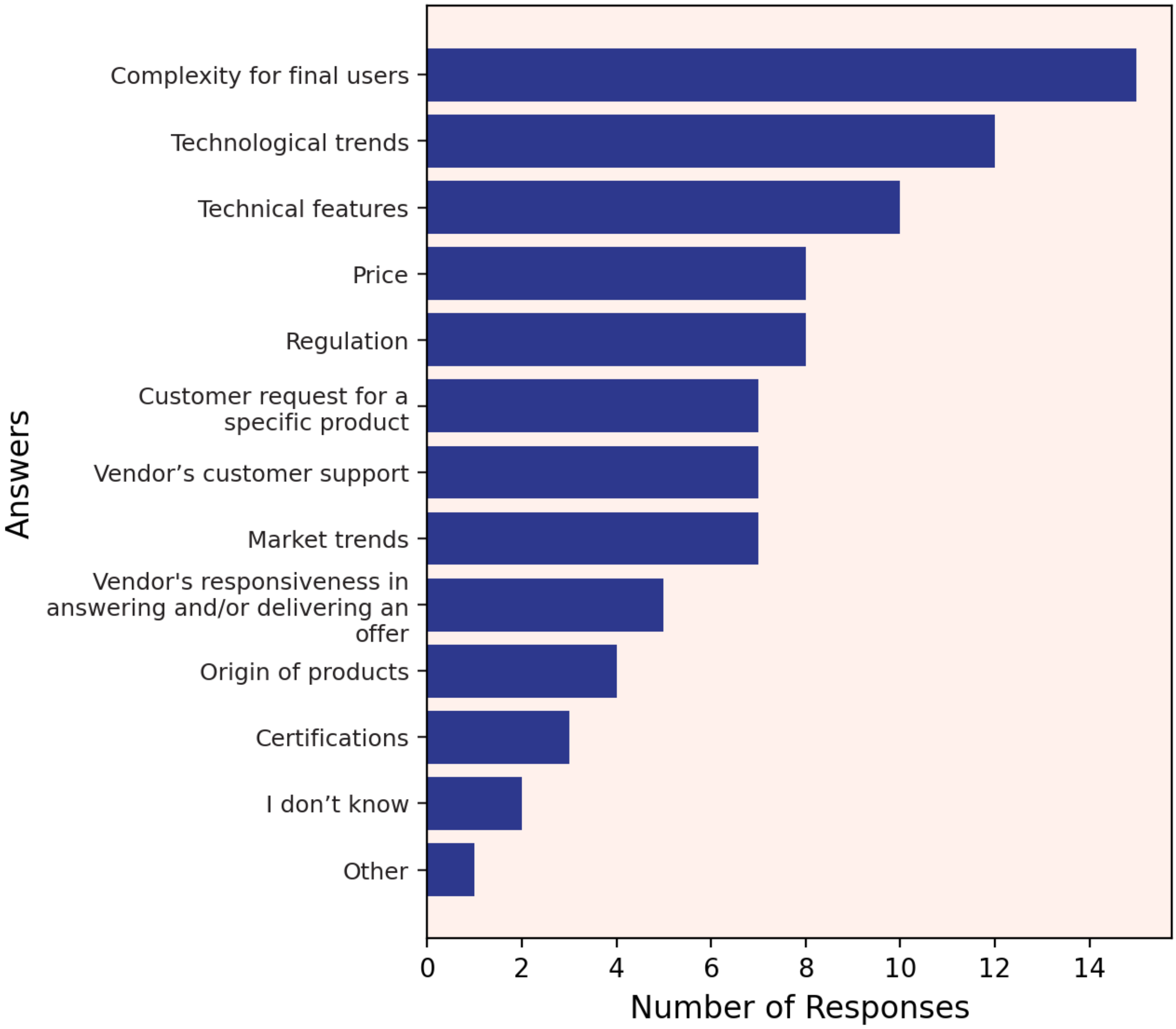


Figure 26: Factors considered in assessing business solutions – insights from the NC3 cybersecurity providers survey

The comment from one respondent in the ‘other’ category of the survey, regarding the factors considered when assessing solutions for business adoption, offer a distinct perspective:

- Preference for Open Source Solutions: The respondent specifies a preference for Free/Libre and Open Source Software (FLOSS) products that can be adapted and modified, with open access to the source code. This indicates a value placed on flexibility, customization, and transparency in software solutions.

Q17 – Is the European origin of a solution, or its association with technological sovereignty, a definitive criterion in the adoption of new solution(s) by your company?

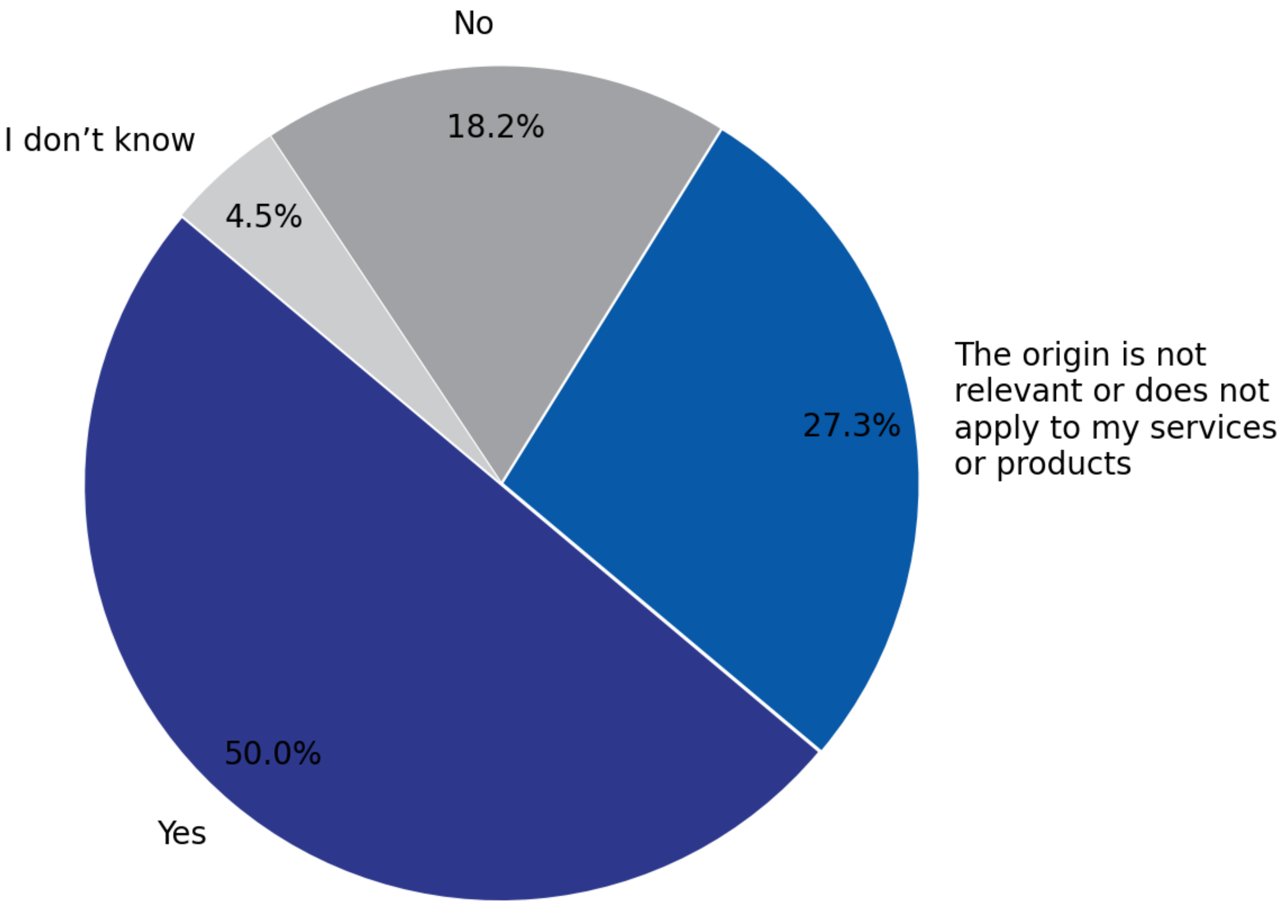


Figure 27: Importance of European origin in solution adoption – responses from the NC3 cybersecurity providers survey

Q18 – Do you think the Luxembourg cybersecurity market is sufficiently open to/welcoming innovation?

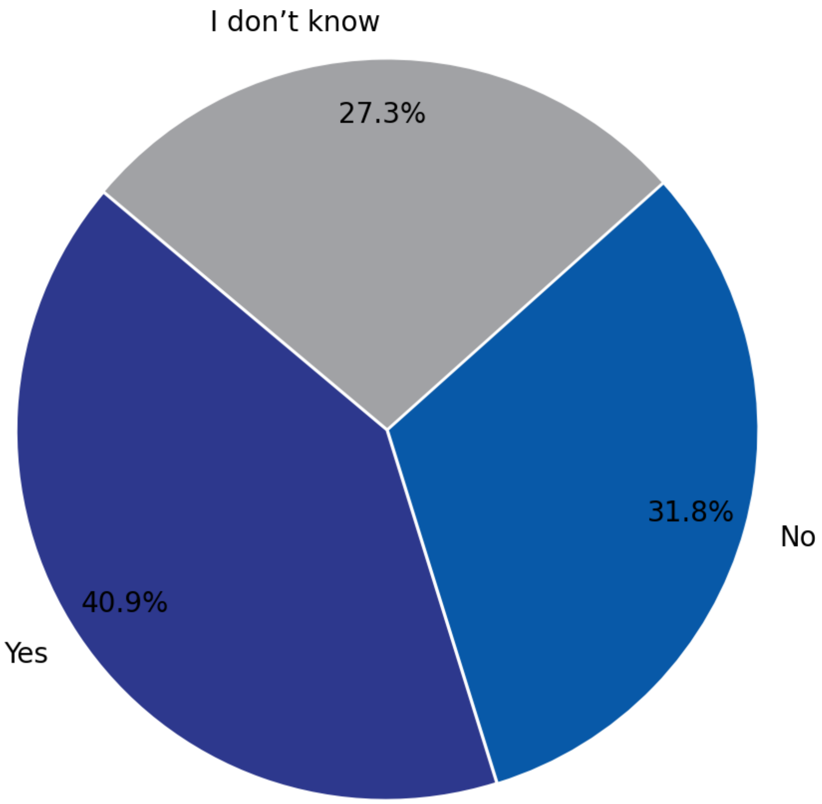


Figure 28: Perceived openness to innovation in Luxembourg’s cybersecurity market – insights from the NC3 cybersecurity providers survey

We asked respondents who expressed dissatisfaction with the market’s openness and welcoming attitude towards innovation the following conditional question: ‘If not, why do you think the Luxembourg cybersecurity market is not sufficiently open to or welcoming of innovation?’ This query revealed several insights into the perceived challenges of the market:

- Lack of Critical Mass for Innovation: One respondent highlighted the issue of not having a critical mass of customers within Luxembourg to amortize the costs of innovation. This suggests a market size limitation, where the small customer base might not justify the investment in innovative cybersecurity solutions.
- Need for Continuous Innovation and Trend Monitoring: Another response emphasized the need for constant monitoring of trends and new features to protect IT assets or data. This points to a dynamic aspect of cybersecurity, where continuous innovation is essential to keep up with evolving threats.
- Market Education and Role of Public Administration: A detailed response pointed out that many firms in Luxembourg are ignorant of cybersecurity. The need for market education and a more proactive role from public administration were stressed. Concerns

were raised about public administration's openness to email encryption and the practice of banks requiring the transmission of confidential information over unsecured channels. This response also highlighted a gap in GDPR protections and suggested revisions to prevent forced transmission of sensitive data through insecure means, along with a call to forbid passport copies to reduce identity theft risks.

- Size and Connectivity Limitations: Another respondent mentioned Luxembourg's small market size and the fact that major cybersecurity decisions for larger groups are often made outside of Luxembourg (in cities like Paris, London, Frankfurt, or in the US). The limited transport connectivity to key European hubs was cited as a barrier for innovative companies trying to expand in this market.
- Skip' Responses: Three responses were 'skip', indicating either a lack of opinion, knowledge, or the desire to not respond to this particular question.

Q19 – Does your organization have a specific approach to integrating open-source solutions into its business model?

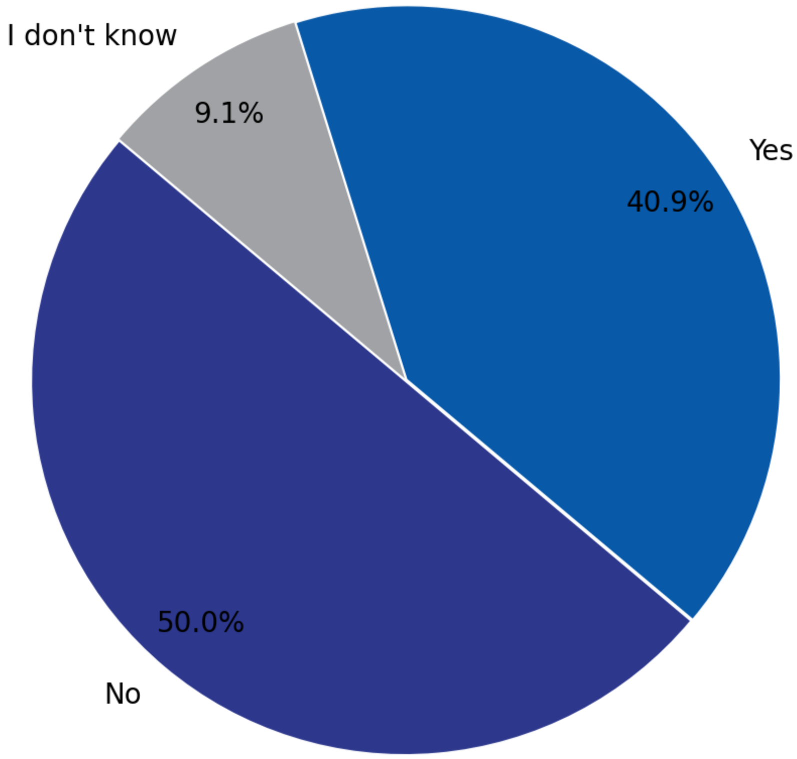


Figure 29: Integrating open-source solutions in business models – responses from the NC3 cybersecurity providers survey

Q20 – Why doesn't your organization integrate open source solutions into its business model?

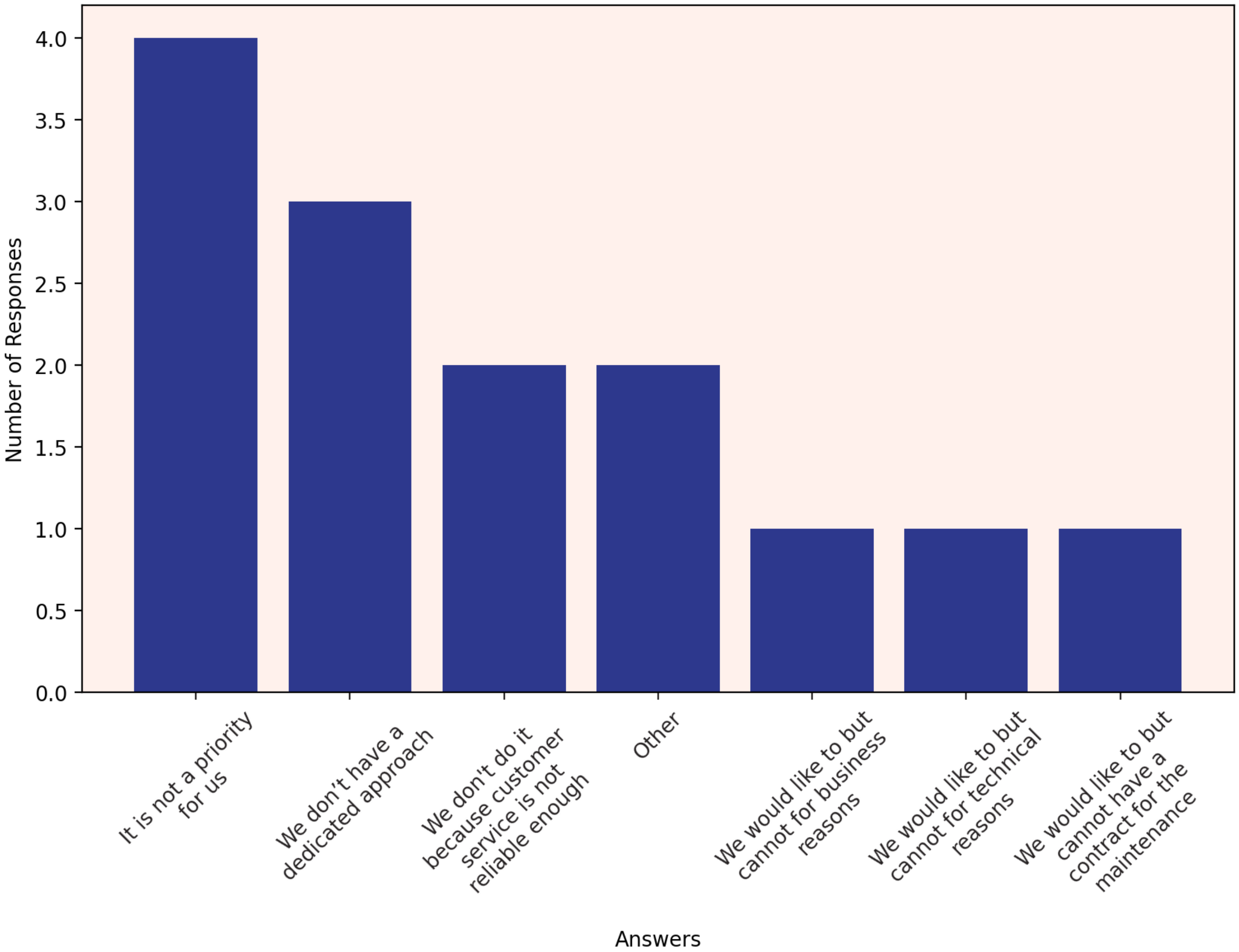


Figure 30: Reasons for not integrating open-source solutions in business models – insights from the NC3 cybersecurity providers survey

The two comments from respondents in the 'other' category of the survey, regarding the integration of open-source solutions into business models, highlight customer preferences and risk management concerns:

- Customer Preferences: One respondent indicates their organization would like to adopt open source solutions, but their customers are resistant to these solutions for various reasons. This suggests that customer attitudes and demands are a significant factor influencing the organization's decision-making.
- Risk Management in Sensitive Industries: The other response comes from an insurance provider, which explains their reluctance to use open source solutions due to the high-risk nature of their work. They handle sensitive information and lack a dedicated risk or cybersecurity team, making the perceived risks of open source software, such as security vulnerabilities or lack of standardized support, more pronounced. Additional-

ly, their small size and the need to comply with strict industry regulations make them cautious about adopting tools that don't offer guaranteed certainty, as is often the case with paid, proprietary tools.

3.7 - Market opportunities

This analysis examines the strategic focus of Luxembourg's cybersecurity providers, particularly their client types and the potential challenges they face in establishing partnerships with multinational subsidiaries.

The survey results regarding the focus on digital or technology-driven enterprises versus less digital intensive and brick-and-mortar businesses are evenly split, with 8 respondents each indicating a focus on digital and a lack of such specific focus. This suggests a balanced approach in the market, catering to both technologically advanced and traditional business sectors.

When asked about issues preventing local IT and cybersecurity solutions from partnering with multinational subsidiaries in Luxembourg, the majority of respondents do not perceive significant barriers, as indicated by 8 respondents. However, 4 respondents believe there are issues, and 7 are unsure. This indicates some level of uncertainty or differing experiences regarding collaborations between local providers and multinational entities.

Regarding the focus on company sizes, a notable number of respondents (8) state that the size of a business is not a relevant metric for their business. This suggests a flexible approach to client engagement, not limited by company size. However, there is also a segment of respondents who specifically do not focus on certain company sizes, including very small businesses (less than 9 or 24 employees) and larger corporations (more than 1000 employees or less than 499 employees). This variation in target market focus reflects the diverse strategies and service capabilities within the Luxembourg cybersecurity industry.

Q21 – Do you focus on digital or technology-driven enterprises rather than non-digital or brick-and-mortar businesses?

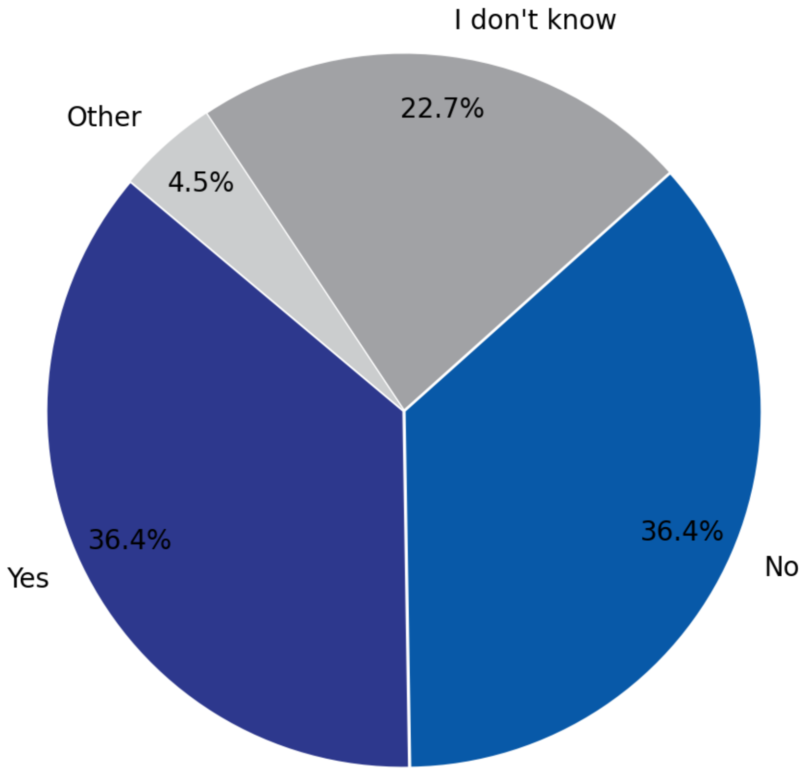


Figure 31: Focus on digital versus brick-and-mortar enterprises – findings from the NC3 cybersecurity providers survey

The comment from a respondent in the 'other' category of the survey, concerning the focus on digital or technology-driven enterprises versus non-digital or brick-and-mortar businesses, offers a specific perspective:

- Cyber Risk Insurance Perspective: The respondent, who appears to be an insurance professional, emphasizes that for products like cyber risk insurance to be relevant, a company must possess a certain level of digital presence or exposure. They state that their company is agnostic to whether a business is primarily online or not. However, they emphasize that offering insurance contracts to a purely brick-and-mortar business that exclusively relies on paper and pencils would be uncommon. This indicates that while their focus is not exclusively on digital enterprises, the nature of their services inherently leans towards businesses with a digital component.

Q22 – From your market experience, do you think that there are issues that prevent Luxembourg's local IT and cybersecurity solutions from partnering with multinational subsidiaries operating within the country?

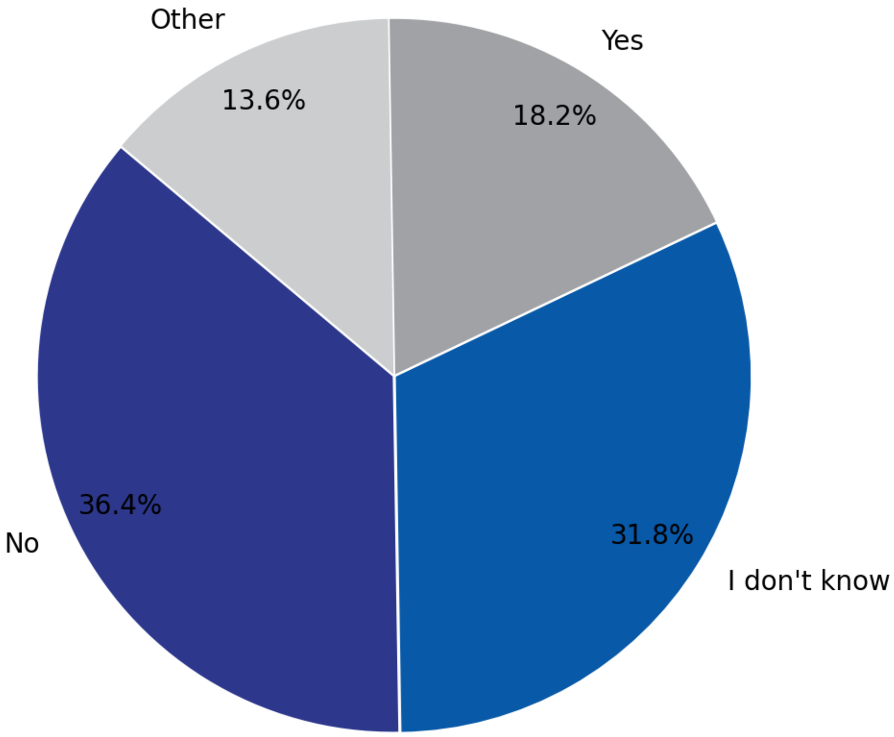


Figure 32: Barriers to partnership between local IT/ cybersecurity solutions and multinational subsidiaries in Luxembourg – insights from the NC3 cybersecurity providers survey

The comments from respondents in the 'other' category of the survey about the challenges that Luxembourg's local IT and cybersecurity solutions face in partnering with multinational subsidiaries reveal a range of insights:

- Difficult to Generalize: One respondent notes that it is difficult to generalize the situation. This response implies that the ability of local IT and cybersecurity firms to partner with multinational subsidiaries may vary widely based on specific circumstances or business models.
- Challenges for Startups in Cybersecurity: Another respondent, identifying as a startup in the cybersecurity space, mentions difficulties in attracting Tier 1/2 enterprises. They propose that providing additional support to small and medium-sized enterprises (SMEs) in the cybersecurity sector could enhance their competitiveness against established multinational players who leverage cybersecurity as a competitive business driver or advantage.
- Promotion and Support for Local Companies: A third response emphasizes the need to

promote and support Luxembourgish companies active in cybersecurity more significantly. This includes suggestions like full and free access to supercomputing resources, permanent access to a team of students from the University of Luxembourg for business-driven projects, and more visibility for Luxembourgish tools as compared to U.S.-based tools.

As a following question we asked to respondents unsatisfied with the market situation: "Given that you perceive obstacles for Luxembourg's local IT and cybersecurity solutions in partnering with multinational subsidiaries, what would you say are the unique considerations or attributes linked to these issues?". The responses provided highlight various considerations and attributes affecting the partnership between Luxembourg's local IT and cybersecurity solutions and multinational subsidiaries:

- Market Size and Cloud Service Restrictions: One response points to the small market size in Luxembourg as a barrier to attracting interest from larger security companies. This respondent also mentions restricted usage of cloud services, which could imply regulatory or market-based limitations impacting the feasibility of partnerships.
- Cost and Resource Availability: Another respondent notes that there is no incentive for multinational subsidiaries to partner with local companies in Luxembourg because:
    - Local services are more expensive than using their own resources or subcontracting to companies in other, cheaper European countries.
    - The tools used by local companies are the same as those used globally (like Nessus, nmap, Kali, Splunk, etc.), suggesting a lack of unique offerings or competitive advantages from Luxembourg-based companies.
- Regulatory Conflicts: A respondent highlights the issue of US regulations undermining EU data protection laws. This suggests a conflict between differing international regulatory standards, creating challenges for local companies in Luxembourg when attempting to partner with multinational entities, especially those based in or operating under US regulations.
- Centralized Decision-Making: The final response indicates that decision-making for multinational subsidiaries is centralized at their headquarters, which are not located in Luxembourg. This centralization means that major transformation decisions are often made with international, rather than local, providers in mind, sidelining local Luxembourg providers.

Q23 – Is there a particular range of company sizes that you do not focus on or exclude from your target market?

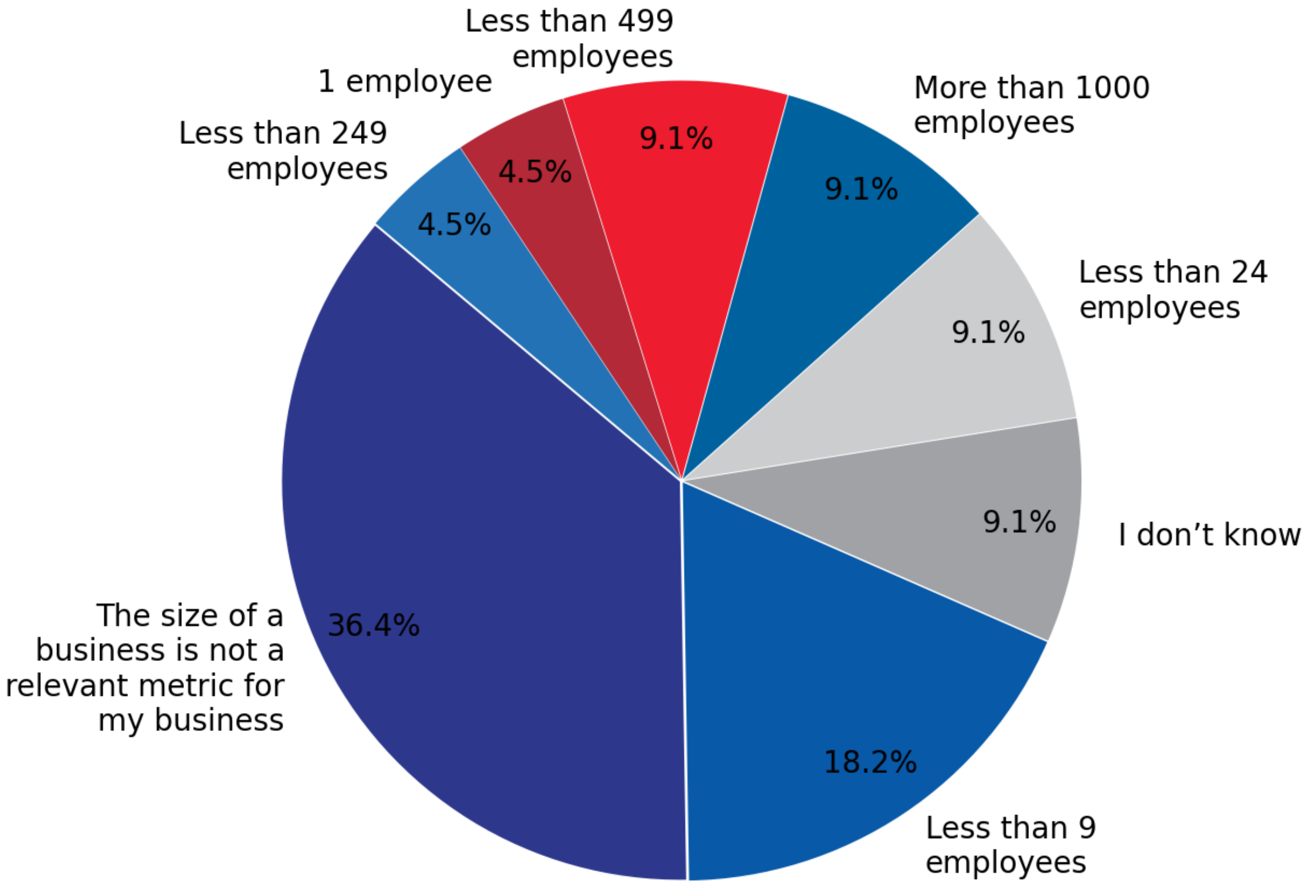


Figure 33: Company size range excluded from target market – findings from the NC3 cybersecurity providers survey

3.8 - Sector specific approach

Our analysis focuses on whether certain sectors in Luxembourg are disproportionately targeted by cyber-attacks, as well as identifying which sectors suffer the most severe consequences from such attacks.

Regarding the targeting of specific sectors, there is a split in perception among the respondents. While 8 believe that certain sectors are more targeted, 5 do not see any particular sector being disproportionately affected, and 9 are unsure.

For the sectors most targeted by cyber-attacks, respondents most frequently identify the financial and insurance activities sector (8 responses), followed by the information and communication sector (5 responses). This indicates a perception that sectors with significant data assets and critical communication infrastructure are at higher risk.

In terms of the severity of consequences from cyber-attacks, the majority of respondents (14) are unsure which sectors suffer the most. However, 6 respondents do perceive that specific sectors face greater consequences. The sectors identified as suffering the most include electricity, gas, steam, and air conditioning supply; construction; and financial and insurance activities. These findings suggest that sectors critical to infrastructure and economic stability may face more significant repercussions from cyber-attacks.

Q24 – Have you noticed that certain sectors in Luxembourg are more targeted by cyber-attacks?

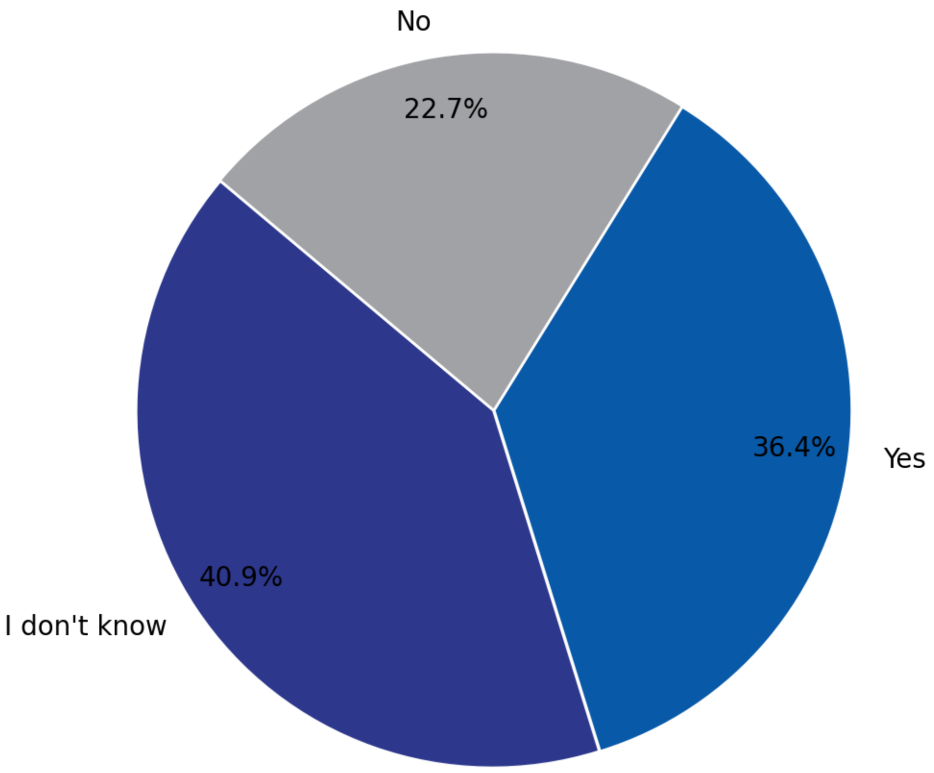


Figure 34: Distribution of answers to the NC3 survey by key drivers in the adoption of cybersecurity services or solutions

Q25 – In your opinion, which three sectors in Luxembourg are most targeted by cyber-attacks?

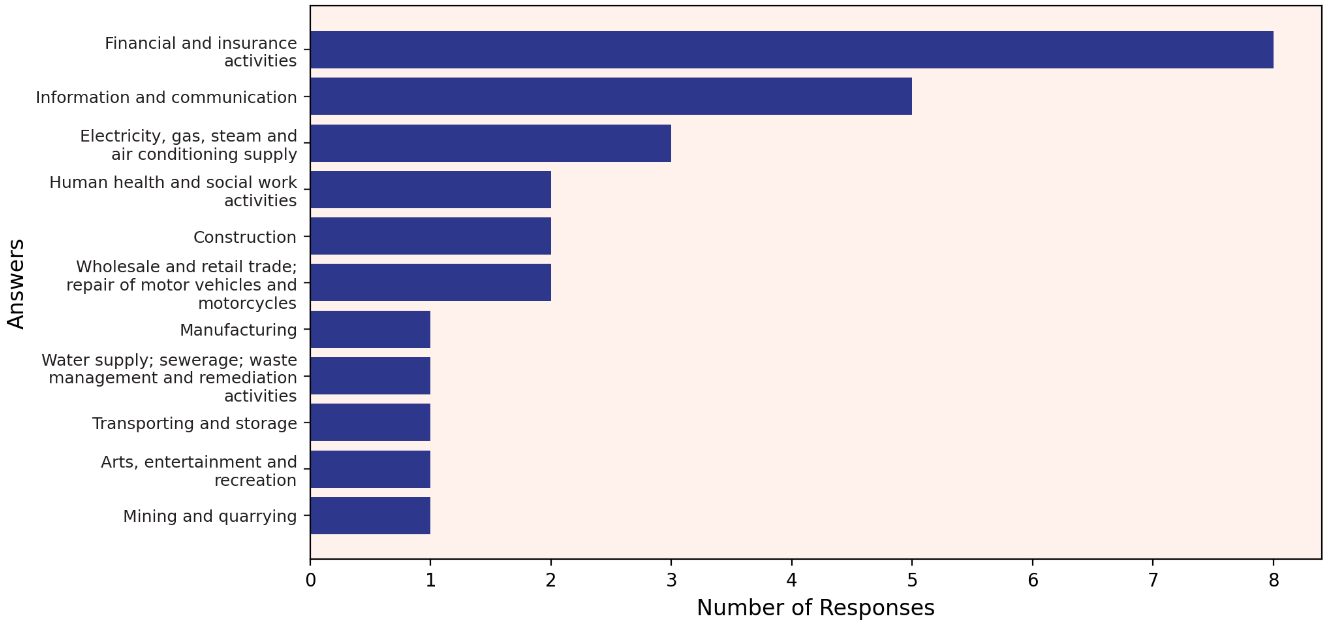


Figure 35: Sectors most targeted by cyber-attacks in Luxembourg – insights from the NC3 cybersecurity providers survey

Q26 – Have you noticed that specific sectors in Luxembourg are suffering greater consequences from cyber-attacks?

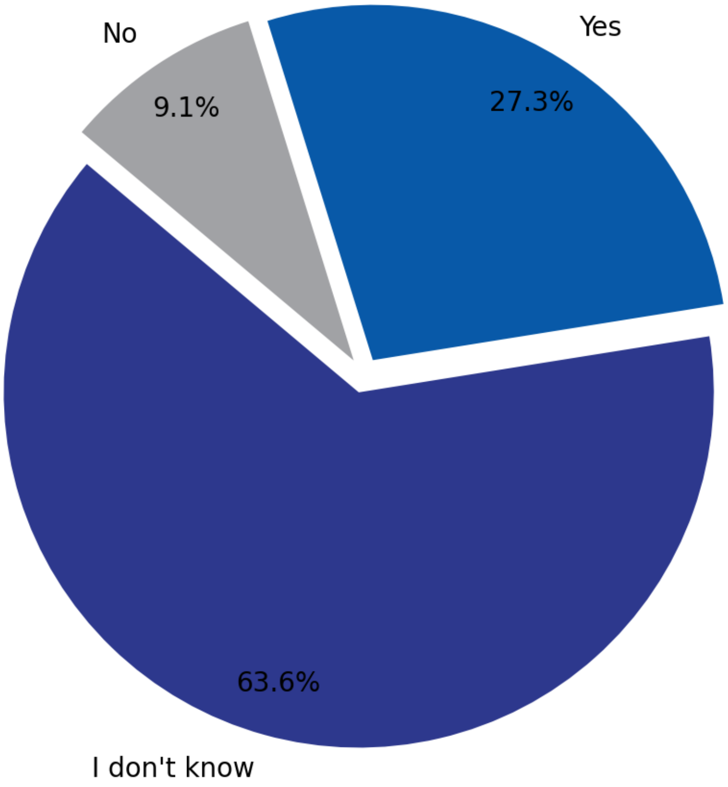


Figure 36: Distribution of answers to the NC3 survey by criteria for evaluating cybersecurity services or solutions

Q27 – In your opinion, which three sectors in Luxembourg are suffering greater consequences from cyber-attacks?

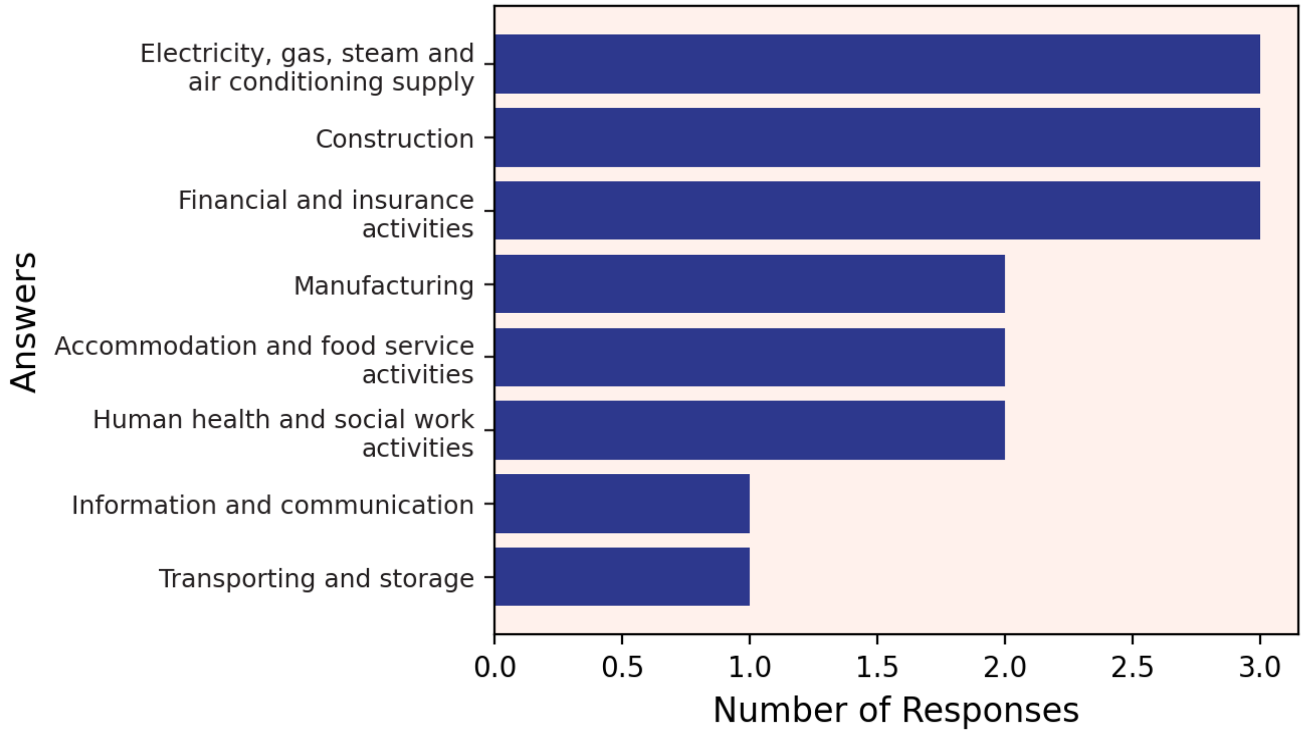


Figure 37: Sectors in Luxembourg suffering most from cyber-attacks – perspectives from the NC3 cybersecurity providers survey

3.9 - Market strengths and weaknesses

This section delves into the perceived strengths and weaknesses of Luxembourg's cybersecurity market, as well as the main concerns regarding its future evolution.

Cybersecurity providers in Luxembourg identify several strengths in the market. The most commonly noted is the strong demand from the financial and banking sector, as indicated by 15 respondents. This is followed by the international orientation of the country and its population (12 responses), a high standard of living (9 responses), and a strategic geographical location (8 responses). These factors suggest that Luxembourg's market is buoyed by robust sectoral demand, international connections, and favorable living conditions.

On the flip side, the perceived weaknesses include a high cost of living, as noted by 16 respondents, and a limited market size, as mentioned by 15 respondents. Other significant concerns include a lack of international exposure, lack of attractiveness for employees, and customers' lack of interest in innovation. These weaknesses highlight challenges related to market expansion, global competitiveness, and innovation adoption.

When considering the future evolution of the market, the respondents express major concerns about a human resources shortage and remote work constraints, each cited by 17 respondents.

The cost of living is also a significant concern (14 responses), along with market regulations and mobility & transportation issues. These concerns suggest apprehension about the market's ability to attract and retain talent, adapt to remote working trends, and navigate regulatory landscapes, all of which are critical for the sustained growth and competitiveness of Luxembourg's cybersecurity sector.

Q28 – From your perspective, what are the strengths of Luxembourg's cybersecurity market?

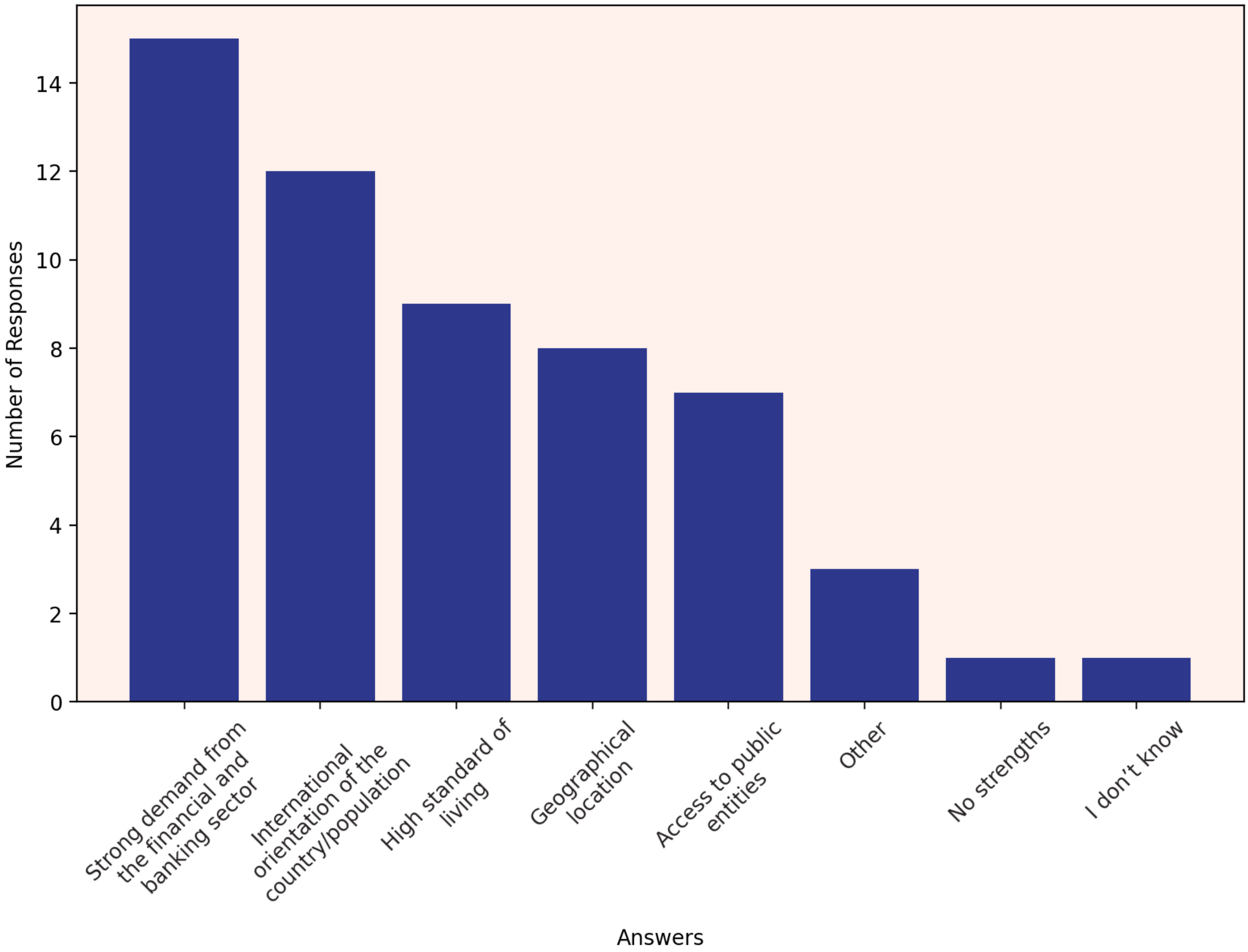


Figure 38: Strengths of Luxembourg's cybersecurity market – insights from the NC3 cybersecurity providers survey

Q29 – From your perspective, what are the weaknesses of Luxembourg's cybersecurity market?

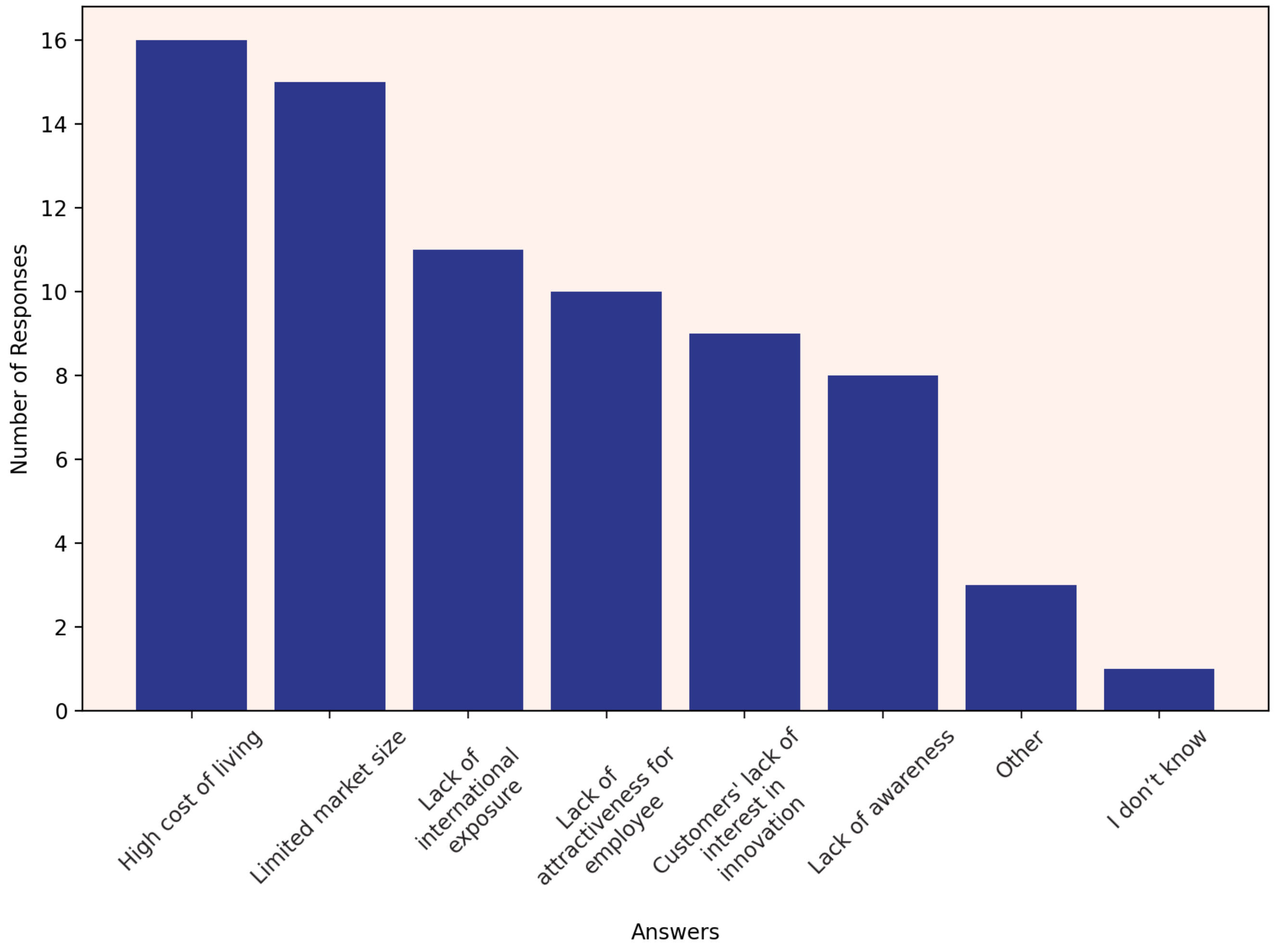


Figure 39: Weaknesses of Luxembourg's cybersecurity market – perspectives from the NC3 cybersecurity providers survey

Q30 – What are your main concerns regarding the evolution of the market?

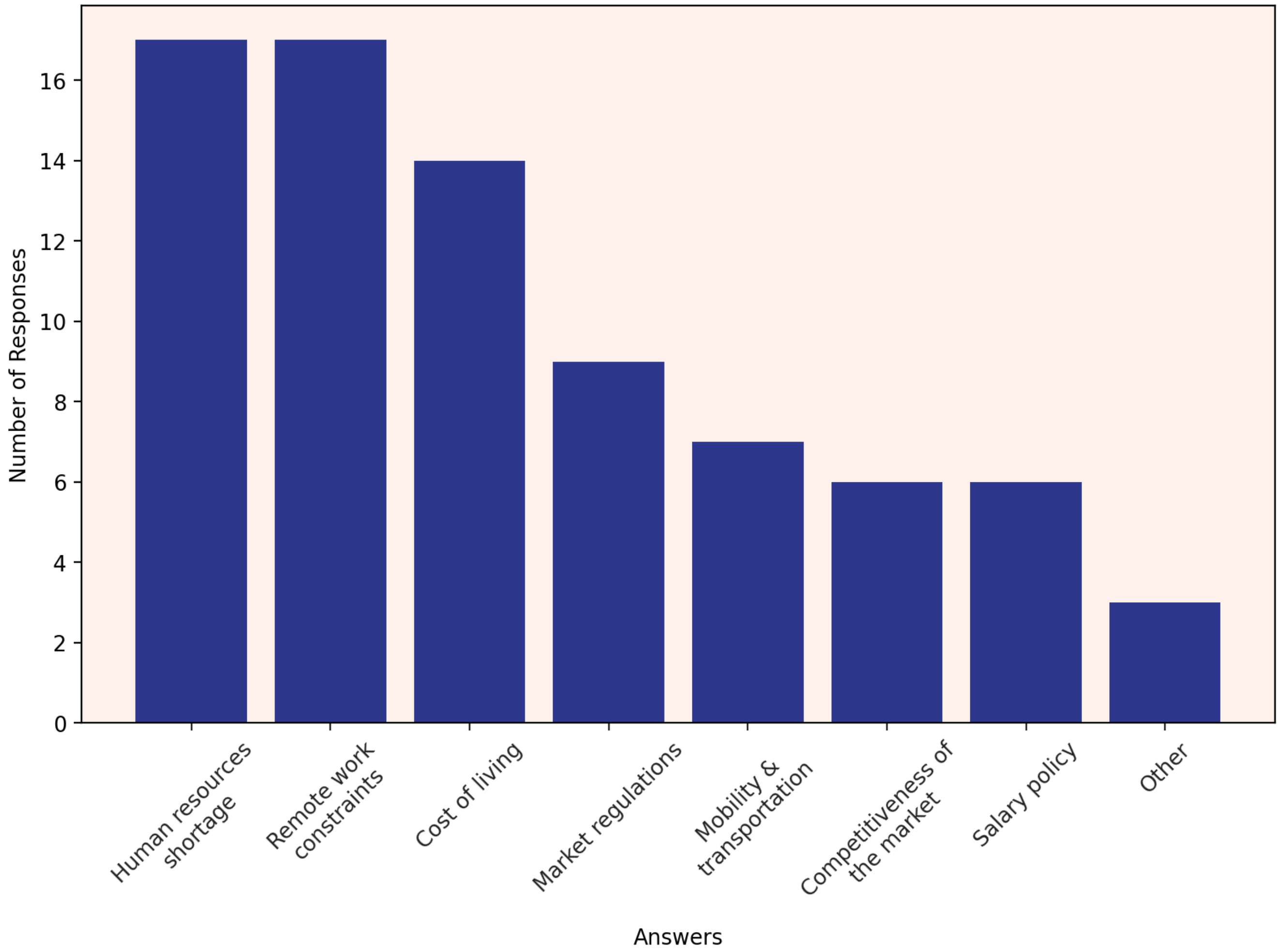


Figure 40: Main concerns about the evolution of the cybersecurity market – responses from the NC3 cybersecurity providers survey

The comments from respondents in the 'other' category of the survey about the main concerns regarding the evolution of the market reveal specific and varied perspectives:

- Competition from Other Countries: One respondent points out that countries like Estonia and Portugal are attracting highly skilled IT and cybersecurity workers with appealing digital nomad packages. This indicates a concern about competition in attracting top talent, suggesting that Luxembourg might need to enhance its offerings to remain competitive in the global market for skilled IT and cybersecurity professionals.
- Influence of US Multinationals and Gaia-X Initiative: Another response highlights concerns about the influence of US multinationals, specifically mentioning the Gaia-X initiative. The respondent feels that the inclusion of these multinationals has rendered the Gaia-X initiative irrelevant. This perspective reflects apprehensions about the dominance of large US tech companies and their impact on European digital and data strategies.

- Lack of Direct Experience with Luxembourg Market: The final response comes from an individual who notes that they currently have no clients headquartered in Luxembourg and, therefore, cannot provide specific insights into the scenario.

3.10 - Shared solutions

In assessing interest in shared solutions among cybersecurity companies and public entities in Luxembourg, the responses reveal a preference for various collaborative cybersecurity measures and services.

The most interest is shown in cloud-based solutions, with 12 respondents indicating a preference for sharing these. This suggests an acknowledgement of the efficiency and scalability benefits that cloud-based cybersecurity solutions can offer. ITSO/CISO as a service and threat intelligence are also highly favored, each garnering interest from 10 respondents. These preferences highlight the growing demand for outsourced cybersecurity leadership and informed, data-driven approaches to threat management.

Incident response and disaster recovery are other areas of interest, with 9 and 8 respondents respectively showing a willingness to share solutions in these domains. This indicates a recognition of the importance of prompt and effective responses to cyber incidents and the need for robust disaster recovery plans. Situational awareness and scalable security training, while less frequently mentioned, still show notable interest with 7 and 4 responses respectively. This reflects an understanding of the need for continuous monitoring of cybersecurity landscapes and the importance of educating staff at scale.

Q31 – Which solutions from the following list are you interested in sharing with cybersecurity companies and public entities in Luxembourg?

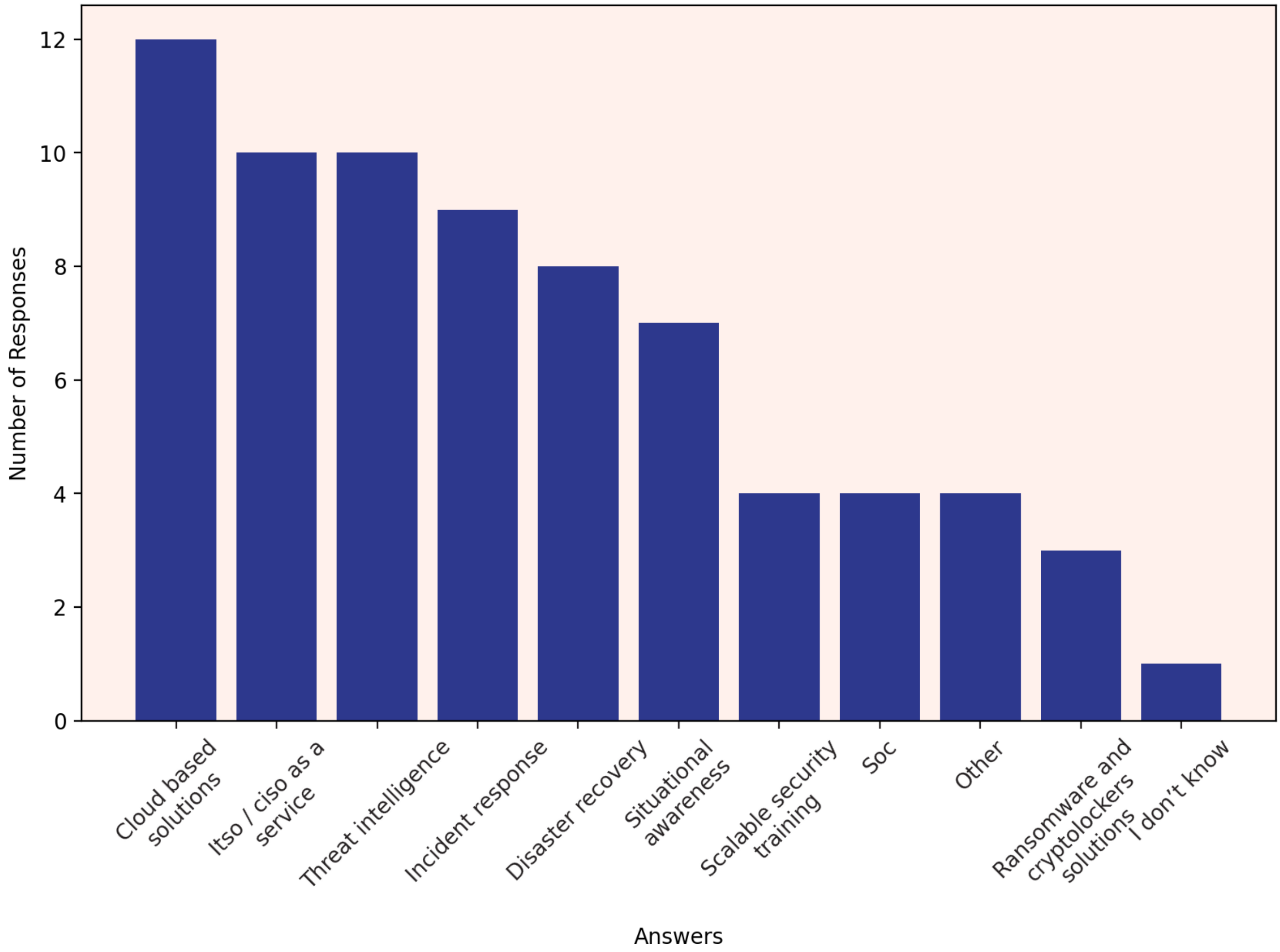


Figure 41: Interest in sharing solutions with cybersecurity companies and public entities in Luxembourg – findings from the NC3 cybersecurity providers survey

The comments from respondents in the ‘other’ category of the survey, concerning their interest in sharing solutions with cybersecurity companies and public entities in Luxembourg, provide unique insights:

- Blockchain – Smart Contract Audit: One respondent is interested in sharing solutions related to Blockchain and Smart Contract Audit, specifically targeting solidity based on Ethereum Virtual Machine (EVM) and specific programming language (e.g. RUST). This indicates a keen interest in the emerging field of blockchain technology and its security aspects, particularly in the area of auditing smart contracts, which are critical components of blockchain systems.
- Cyber Governance Risk and Compliance Tooling: Another response mentions interest in Cyber Governance Risk and Compliance tooling, with a specific mention of DORA (Digital Operational Resilience Act)[29] compliant tooling. This reflects a focus on regula-

[29] The Digital Operational Resilience Act (DORA) - Regulation (EU) 2022/2554, Source: EUR-Lex, Last A cessed: 23/01/2024, Link: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595

tory compliance and the management of digital risks, aligning with emerging European Union regulations that aim to enhance digital operational resilience.

- Offensive Security (Pentest, etc.): A respondent expressed interest in sharing solutions related to Offensive Security, including penetration testing. This shows an awareness of the importance of proactive security measures, where simulating cyberattacks (penetration testing) is utilized to identify and rectify vulnerabilities.
- Cyber Insurance as a Mutual: The final response highlights offering cyber insurance in a mutual structure, allowing members to share intelligence while also benefiting financially from an insurance policy. This approach suggests a collaborative model where members not only gain insurance protection but also contribute to and benefit from shared cybersecurity intelligence.

3.11 - Public services

In evaluating the role of government and public agencies in Luxembourg's cybersecurity ecosystem, the responses indicate a prevailing expectation for increased support and promotion.

The majority of respondents (12) believe that the government and its agencies should do more to bolster Luxembourg's cybersecurity environment. This suggests a perceived need for greater involvement or initiative from public authorities in this sector.

When asked about specific areas that should receive particular attention for greater support or promotion, there is a three-way tie among private-public partnerships, support for the growth of security SMEs, and funding and incentives, each receiving 7 mentions. This highlights a desire for stronger collaboration between the private and public sectors, targeted support for small and medium-sized enterprises in the cybersecurity field, and financial incentives to stimulate growth and innovation.

Other areas identified for enhanced focus include international collaboration and a more robust regulatory framework, each noted by 6 respondents. Additionally, marketing and events, research and development support, and private sector collaboration are also seen as important, though mentioned less frequently. These areas collectively emphasize the need for a comprehensive approach that includes global cooperation, regulatory clarity, and concerted efforts in marketing, research, and private sector engagement to strengthen Luxembourg's position in the cybersecurity landscape.

Q32 – Do you expect the government and its agencies to do more to support or promote Luxembourg's cybersecurity ecosystem?

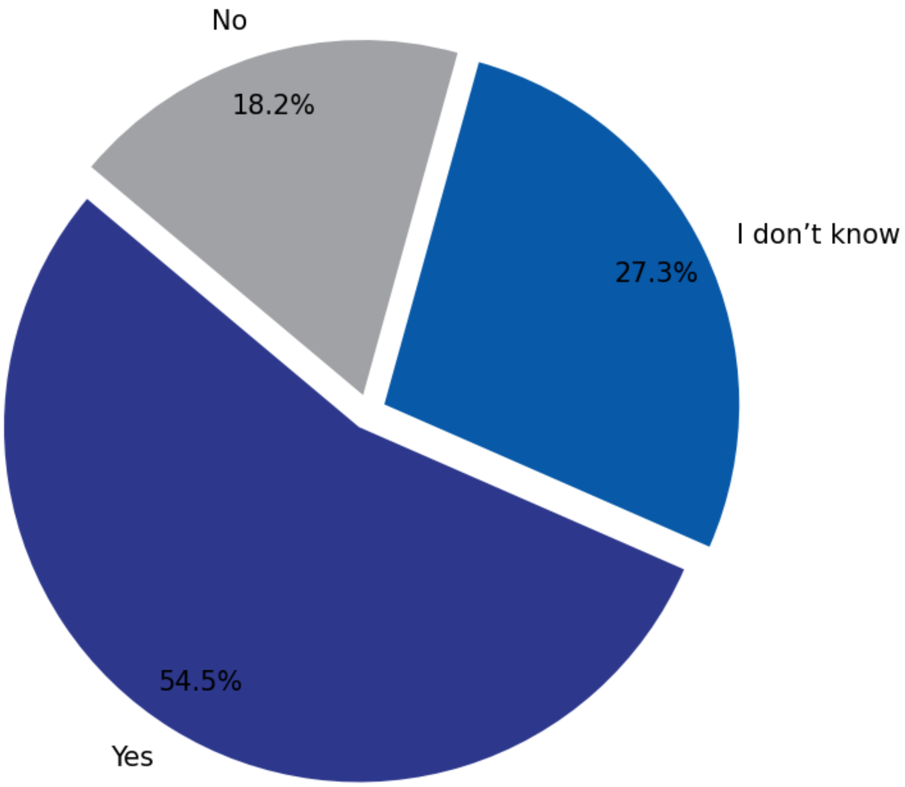


Figure 42: Expectations for government support in Luxembourg's cybersecurity ecosystem – insights from the NC3 cybersecurity providers survey

Q33 – Given your expectation of greater support or promotion of Luxembourg's cybersecurity ecosystem by the government and its agencies, what specific areas do you think should receive particular attention?

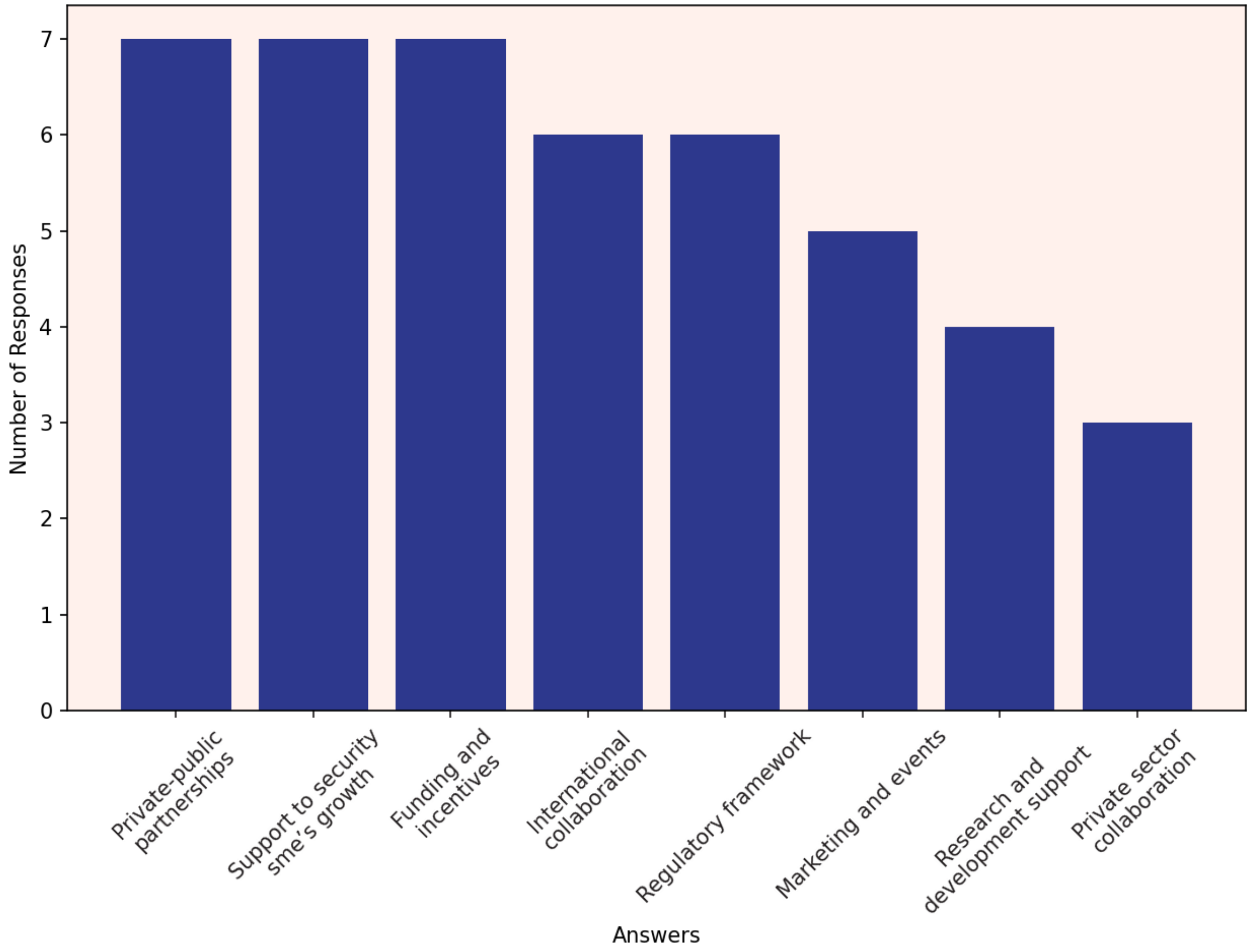


Figure 43: Suggested areas for government support in Luxembourg's cybersecurity ecosystem – perspectives from the NC3 cybersecurity providers survey

3.12 - Feedback from respondent

The survey feedback from the respondents can be categorized into several key themes:

- **General Feedback**: A majority of respondents (12 out of 22) indicated no additional comments or concerns, suggesting either satisfaction with the current state of affairs or a lack of further insights to share.
- **Support for SMEs:**
  - Supporting SMEs: One respondent emphasized the importance of supporting SMEs in cybersecurity, suggesting that bolstering SMEs can enhance the overall safety of the ecosystem.
  - Cybersecurity Not a Priority for SMEs: Another respondent noted that cybersecurity is often not a priority for SMEs and without legal obligations, they are unlikely to

invest in it.

- **Evolution of Technology and Cybersecurity:**
  - One respondent highlighted the exponential evolution of technology, particularly with the advent of 5G and quantum computing. They pointed out that these advancements could lead to significant cyber threats impacting the profit and loss, as well as the reputation, of firms in the digital world.
  - They also mentioned that Luxembourg, positioning itself as a center of excellence for cybersecurity, needs to focus on identifying, attracting, retaining, and promoting talents who can contribute to cybersecurity and, by extension, to Luxembourg's reputation as a secure financial center.
- **Promotion of Local Cybersecurity Companies:**
  - One respondent expressed interest in being promoted as a local cybersecurity company, indicating a desire for greater visibility and recognition within the ecosystem.
- **Concerns About Competition with Public Institutions:**
  - A respondent expressed confusion about why some publicly funded institutions are acting as competitors in the market, indicating a potential concern about the role and impact of public entities in the cybersecurity space.
- **Government Support for Small and Medium Cybersecurity Businesses:**
  - There was a suggestion that the government should support small to medium-sized cybersecurity businesses to help them compete with larger entities in Luxembourg, emphasizing that smaller startups and companies are often more security-driven than profit-driven.

4 – Key Findings of the 2023 Cybersecurity Ecosystem Study

Luxembourg's Evolution into a Cybersecurity Hub

- Luxembourg has significantly advanced its cybersecurity infrastructure, aligning with the OECD's 'Towards a Culture of Security' guidelines in terms of awareness, education, risk management, collaboration, and legal framework.
- The cybersecurity sector has become an integral part of Luxembourg's digital transformation and economic growth.
- Global Cybersecurity Maturity
- Recognized in the Global Cybersecurity Index, Luxembourg ranks highly in Europe for cybersecurity measures, especially in legal, technical, and cooperative aspects.
- The 2020 Global Cybersecurity Index score indicates potential for further improvement in organizational measures.

CYBERSECURITY Luxembourg Initiative and Ecosystem

- Launched in 2019, this initiative strengthens public-private cooperation in cybersecurity, aligning with the national cybersecurity strategy.
- A comprehensive mapping and interactive dashboard have been developed to enhance the cybersecurity sector visibility and collaboration.
- The ecosystem comprises 311 companies, including 70 startups, with 85 focusing primarily on cybersecurity.

Market Dynamics and Financial Analysis

- The European cybersecurity market is projected to experience significant growth, driven by digital transformation, IoT, and emerging cyber risks.
- A detailed financial analysis of Luxembourg's cybersecurity sector reveals disparities in profit and loss among companies and a concentration of smaller-sized entities.
- The market faces challenges in assessment due to foreign company dominance and limited public financial reporting.

Market Trends

- The market is characterized by diverse revenue-generating activities, with consulting, professional services, and business continuity services as top drivers.
- There's a mixed approach towards open-source solutions and innovation, with concerns about market education, public administration's role, GDPR gaps, and centralized decision-making.

Public Services and Government Role

- There is a prevailing expectation among companies in the ecosystem for increased government support to strengthen Luxembourg's cybersecurity ecosystem.
- Respondents suggest focusing on private-public partnerships, support for security SMEs, and funding and incentives to improve the level of cybersecurity maturity of these entities.

Sector-Specific Approach

- Respondents identify financial and insurance activities as the most targeted sectors by cyberattacks.Sectors critical to infrastructure and economic stability may face more severe consequences from cyberattacks.

Market Strengths and Weaknesses

- Strengths: Strong demand from the financial sector, international orientation, high standard of living, and strategic location.
- Weaknesses: High cost of living, limited market size, lack of international exposure, and challenges in innovation adoption.

Future Concerns and Opportunities

- Major concerns include human resources shortages, remote work constraints, cost of living, and regulatory challenges.
- Opportunities for growth and improvement are seen in enhancing government support, promoting local cybersecurity companies, and addressing challenges faced by startups and SMEs in cybersecurity.

5 – Conclusion and future directions

The recent market intelligence report on SMEs[30] has been substantially validated by feedback from cybersecurity providers, revealing crucial insights into the current landscape and future directions of the cybersecurity sector in Luxembourg.

Validation of previous findings

The study's findings confirm that SMEs exhibit varying levels of cybersecurity maturity, largely influenced by their experiences with cyber threats. This variation underscores the necessity of tailored cybersecurity approaches, accommodating the diverse needs and contexts of SMEs. Furthermore, the importance of financial and legal incentives emerges as a key driver in promoting proactive cybersecurity measures among SMEs. This suggests a significant role for supportive policy frameworks and incentive structures in enhancing cybersecurity readiness among SMEs.

Anticipated impact of the NIS 2 directive

The NIS 2 directive[31] is expected to have a significant impact on Luxembourg's cybersecurity ecosystem and market. It will likely introduce stricter cybersecurity regulations, driving increased demand for cybersecurity services and solutions. This presents business opportunities for cybersecurity companies, particularly those offering consulting, technology solutions, and training services.

Emphasis on human resources

One key theme emerging from the study is the critical role of human resources in cybersecurity. The sector faces a noticeable skills gap, emphasizing the need for focused efforts in talent acquisition, retention, and development. The effectiveness of digital and cybersecurity strategies relies heavily on the availability and expertise of human resources. Therefore, talent management becomes a strategic priority to meet the evolving demands of NIS 2 compliance.

Potential pathways to address the cybersecurity skills gap

As Luxembourg adapts to the new regulatory landscape, there may be a surge in cybersecurity innovation and collaboration, with the government likely investing in initiatives to support compliance. Smaller businesses, particularly SMEs, may seek assistance from specialized cy-

[30] A Comprehensive Market Study on Cybersecurity Challenges and Opportunities in Luxembourg's SME sector, Last Accessed: 23/01/2024 Link: https://observatory.nc3.lu/market-intelligence-library/report-2023/

[31] NIS 2 Directive, Source: EUR-Lex, Last Accessed: 23/01/2024, Link: https://eur-lex.europa.eu/eli/dir/2022/2555

bersecurity firms to navigate the regulatory requirements. This could lead to the growth of a robust cybersecurity workforce in Luxembourg, addressing the skills gap and ensuring the country's competitiveness in the digital era.

Future research focus

Given these insights, future studies will concentrate on the human element of cybersecurity. This includes exploring effective talent acquisition strategies to attract skilled professionals in a globally competitive market, developing retention mechanisms to maintain top talent, and addressing skill gaps through targeted education and training initiatives.

nc3.lu
National Cybersecurity
Competence Center
LUXEMBOURG

nc3
Cybersecurity
Observatory

Published by the Luxembourg House of Cybersecurity
May 2024