A Comprehensive Market Study on Cybersecurity Challenges and Opportunities in Luxembourg's SME Sector

December 2023

Available for download on:

nc3
Cybersecurity
Observatory

Published by:

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 ABBL, the Chambre of Commerce, the Chamber of Trades, the Federation of Craftsmen, the FEDIL, the House of Entrepreneurship, the House of Startups. We also extend our gratitude to the Ministry of the Economy of Luxembourg, our colleagues of the Luxembourg House of Cybersecurity and all the SMEs that participated in our survey and focus group for their invaluable contributions to the mission of the National Cybersecurity Competence Center.

ABBL

CHAMBER
OF COMMERCE
LUXEMBOURG
POWERING BUSINESS

CHAMBRE
DES MÉTIERS
LUXEMBOURG

FEDERATION
DES ARTISANS

FEDIL
The Voice of Luxembourg's Industry

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Économie

HOUSE OF
ENTREPRENEURSHIP
powered by the Luxembourg Chamber of Commerce

HOUSE OF STARTUPS
powered by the Luxembourg Chamber of Commerce

Table of Contents

A Comprehensive Market Study on Cybersecurity Challenges and Opportunities in Luxembourg's SME sector

List of acronyms and organizations mentioned in this study

- ABBL – Luxembourg Bankers' Association
- AI – Artificial Intelligence
- CIRCL – Computer Incident Response Center Luxembourg
- CISO – Chief Information Security Officer
- CNPD – National Commission for Data Protection
- CSA – Cybersecurity Act
- CSIRT – Computer Security Incident Response Team
- CSSF – Financial Sector Supervisory Commission
- DESI – Digital Economy and Society Index
- DPO – Data Protection Officer
- ENISA – European Union Agency for Cybersecurity
- ESRIC – European Space Resources Innovation Centre
- EU – European Union
- FEDIL – Organisation of Luxembourg's Industry
- GDPR – General Data Protection Regulation
- ICS – Industrial Control Systems
- IEC – International Electrotechnical Commission
- IGSS – Social Security General Inspectorate
- ILR – Luxembourg Regulatory Institute
- IP – Internet Protocols
- ISO – International Organization for Standardization
- IT / ICT – Information Technology / Information and communication technology
- LHC – Luxembourg House of Cybersecurity
- LHoFT – Luxembourg House of Financial Technology
- LLM – Large Language Model
- NACE – Statistical classification of economic activities
- NC3 – National Cybersecurity Competence Center Luxembourg
- NIS – Security of network and information systems
- OECD – Organisation for Economic Co-operation and Development
- OT – Operational technology
- PEST – Political, Economic, Sociological, and Technological
- SCADA – Supervisory Control and Data Acquisition
- SME – Small and medium-sized enterprises
- STATEC – National Institute for Statistics and Economic Studies
- VPN – Virtual Private Network

Executive summary

In today's digital era, Small and Medium Enterprises (SMEs) are a double-edged sword. They significantly contribute to employment and GDP but are vulnerable to cybersecurity threats due to limited resources. From freelancers using third-party services to mid-sized firms with in-house IT, SMEs represent a wide range of different companies with their own needs. Cybersecurity readiness across SMEs is far from uniform, influenced by size, funding, and tech adoption levels. Amidst a push towards digital transformation from the market and with support from public authorities, SMEs are adopting more complex technologies, potentially increasing their exposure to cyberattacks. Given that Luxembourg is a small country with only a few sources regarding its cybersecurity market, the Luxembourg House of Cybersecurity has established a market intelligence observatory to share insights with local stakeholders and international partners. This study represents the first undertaking of this newly created platform.

Objectives of this study:

- Gain a deep understanding of the cybersecurity challenges facing SMEs in Luxembourg.
- Identify potential gaps in cybersecurity measures within these SMEs.
- Gather insights on the support mechanisms and resources that the NC3 can offer to enhance SME cybersecurity practices.
- Develop targeted cybersecurity programs and initiatives aimed at fortifying SMEs against cyber threats.

Research methodology:

- Reviewed existing literature and data sources as a foundation for the study.
- Applied a PEST (Political, Economic, Sociological, and Technological) matrix to explore external factors affecting cybersecurity for SMEs in Luxembourg.
- Generated research hypotheses and formulated them into survey questions.
- Administered an online survey in three languages to collect firsthand data from SMEs and gather new market statistics.
- Conducted focus groups with SME owners, managers, and IT professionals for detailed insights related to the survey.
- Received peer and expert reviews from the Luxembourg House of Cybersecurity.

Perceived needs of Luxembourg SMEs:

- **Cybersecurity as a key driver for digitization:** Recognizing the interdependence of cybersecurity and the digitization of SMEs is crucial. As SMEs increasingly rely on digital tools and platforms to enhance their operations and reach, they inadvertently expose themselves to various cyber threats. Cybersecurity, therefore, becomes a foundational element in their digital transformation journey.
- **Cost-effective, automated, tailored solutions:** There is a lack of affordable and tailored cybersecurity solutions specifically designed for SMEs with limited resources. Off-the-shelf solutions might not address the unique needs and constraints of smaller businesses.
- **Budget considerations for cybersecurity:** Financial constraints often dictate the direction of organizational strategies, especially for SMEs. Budgeting plays a pivotal role in determining the extent and nature of cybersecurity measures an organization can implement. Without adequate budgeting for cybersecurity, SMEs risk being under-protected, leaving them vulnerable.
- **Persistent cybersecurity skills gap:** SMEs often lack the in-house skills to effectively manage and implement cybersecurity measures, and to assess their needs for new solutions. The result is a gap between awareness and implementation as well as a feeling of “blind trust” in the solution providers.
- **Ensuring compliance for SMEs through supportive platforms:** Navigating the complex landscape of cybersecurity regulations, standards, and frameworks is particularly challenging for SMEs. Many are unsure about the specific requirements they need to fulfill.
- **Strengthening supply chain security by engaging non-expert contacts in SMEs:** SMEs, often integral to expansive supply chains, are vulnerable to cyber risks emanating from third-party ties and dependencies. More critically, the primary contact in these SMEs is seldom a cybersecurity or IT expert, making effective communication during crises imperative.

Strategic recommendations for enhancing public initiatives:

- **Incubation and support companies specializing in compliance and automation:** Promote the growth of companies focusing on cybersecurity solutions tailored for SMEs by emphasizing compliance and harnessing open-source large language model (LLM) technology. This approach ensures cost-effective adaptations to the diverse and intricate SME environments, making otherwise unfeasible solutions profitable.

- **Educational imperatives in cybersecurity:** Begin cybersecurity education in schools, underscoring its growing importance. Design and support versatile educational programs such as the Digital Learning Hub[1] that range from awareness to technical skills, and are aimed at everyone from students to business leaders, to integrate cybersecurity into a lifelong learning approach to protecting individuals and organizations.
- **Regulatory simplification advocacy:** Collaborate with regulatory bodies to advocate for streamlined and SME-friendly cybersecurity regulations. Work towards harmonizing national and European standards to simplify compliance efforts. Leverage the work done by the National Commission for Data Protection (CNPD) and the Institut Luxembourgeois de Régulation (ILR).
- **Centralized contact directory for breaches:** Initiate a directory for individuals to contact during cybersecurity incidents, streamlining the flow of crucial threat information within the CERT-LU[2] community and emphasizing knowledge-sharing over commercial goals.
- **Facilitating SME awareness of their needs with trustworthy intermediaries:** Employ trusted entities, such as professional organizations and government bodies, to connect SMEs with cybersecurity firms tailored to their specific needs. Establish a link between the Cybersecurity Luxembourg ecosystem platform[3] and the Fit4Cybersecurity[4] tool to assess company needs and facilitate connections with local providers of cybersecurity services and products.
- **Jumpstarting security measures for SMEs through financial aid:** Develop the "Fit4Cybersecurity"[5] program for SMEs with a public-private partnership, backed by the Chamber of Commerce. This program aids SMEs in assessing their IT and cybersecurity needs and enhancing protection. Consider partial subsidies for SMEs' expenses and offer financial incentives to encourage investment in vital cybersecurity technologies and services.

[1] About Digital Learning Hub, Last Accessed: 08/11/2023, Link: https://dlh.lu/about-us/

[2] CERT-LU, Source: CERT-LU, Last Accessed: 08/11/2023, Link: https://cert.lu/

[3] Private sector dashboard, Source: CERT-LU, Last Accessed: 08/11/2023, Link: https://www.cybersecurity.lu/ecosystem?tab=private-sector

[4] Fit4Cybersecurity online survey, Source: NC3, Last Accessed: 08/11/2023, Link: https://fit4cybersecurity.nc3.lu/

[5] Poser les fondations d'une "Data-driven Economy" compétitive et innovante, Source: Luxembourg Chamber of Commerce, Last Accessed: 26/10/2023, Link: https://www.cc.lu/toute-linformation/publications/detail/elections-2023-poser-les-fondations-dune-data-driven-economy-competitive-et-innovante?tx_ccpublications_publications%5Bpage%5D=1&cHash=efcc92a278e9b20161b9394843071dde

A Comprehensive Market Study on Cybersecurity Challenges and Opportunities in Luxembourg's SME sector

1 – Study on the cybersecurity needs of Luxembourg SMEs

1.1 – Study rationale and objectives

The Luxembourg House of Cybersecurity is helping businesses in the country get better at defending against online threats. As part of this effort, its department, the National Cybersecurity Competence Center (NC3) is conducting a detailed study to really understand what small and medium-sized businesses need for cybersecurity.

This needs assessment of SMEs represents the initial phase of a broader study focused on the national cybersecurity market. The goal is to evaluate the alignment between solution providers and their clientele.

This study is the fruit of collaboration between the Data For Research, Innovation, and Governance (D4RIG) team of the National Cybersecurity Competence Center with experts of the Luxembourg House of Cybersecurity, the ABBL, the Chamber of Commerce, the Chamber of Trades, the Federation of Craftsmen, the FEDIL, the House of Entrepreneurship, the House of Startups and the Ministry of the Economy.

Study Objectives:

1. Gain a deep understanding of the cybersecurity challenges facing SMEs in Luxembourg.
2. Identify potential gaps in cybersecurity measures within these SMEs.
3. Gather insights on the support mechanisms and resources that the NC3 can offer to enhance SME cybersecurity practices.
4. Formulate recommendations on cybersecurity programs and initiatives aimed at fortifying SMEs against cyber threats.

Research Methodology:

1. Preliminary Research: An in-depth examination of data collected from statistical agencies, research organizations and open platforms, aimed at providing an understanding of the market landscape that enables research hypotheses to be formulated.
2. PEST (Political, Economic, Sociological, and Technological): This matrix was

employed to investigate external factors that influence the cybersecurity landscape for Luxembourg's SMEs and to structure the analysis of the report.

3. Survey: This tool was used to generate statistics from the responses of various SMEs in Luxembourg to questions designed to complement pre-existing sources.
4. Focus Group: An open and guided discussion was conducted with carefully selected SME owners, managers and IT professionals, representing various industries in Luxembourg.
5. Review by peers: Validation of the report by cybersecurity experts of the Luxembourg House of Cybersecurity.

1.2 – Structure of the study

This report shares the results of research into the cybersecurity challenges facing SMEs in Luxembourg. In the second part, we share the work done to gather data on the existing knowledge available on this topic, which has been brought together as part of a high-level analysis on political, economic, sociological and technological aspects. This initial analysis has enabled us to highlight some missing data points, which we have attempted to fill using a survey, the results of which are shared in the third part, and by discussing with business representatives in a focus group, the summary of which is shared in the fourth chapter. We have also highlighted the key findings in terms of perceived needs and recommendations in the last part of the report of this study.

1.3 – Definition of the object of study

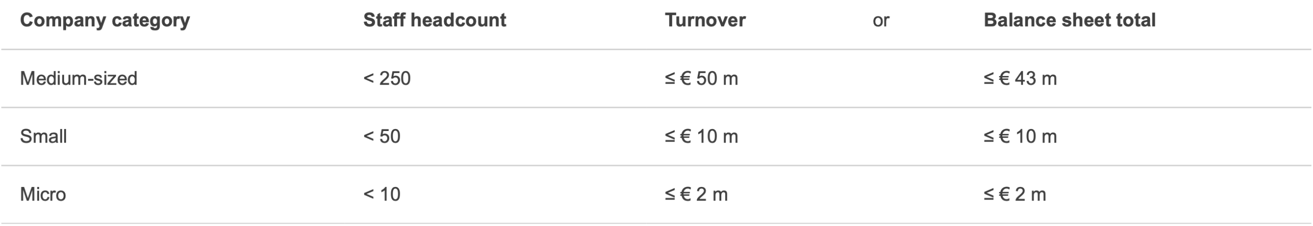
To define the focus of our study while respecting common terminology that could be used and shared with other National Cybersecurity Competence Centers,[6] we have decided to adopt the European definitions of SMEs and sectors of activity (NACE CODE). The European Commission has published a precise definition of company categories as part of its work on the European single market in Recommendation EU 2003/361:[7]

The main factors determining whether a company is an SME are:

[6] National Coordination Centres, Source: European Cybersecurity Competence Centre and Network, Last Accessed 25/10/2023, Link: https://cybersecurity-centre.europa.eu/nccs_en

[7] Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises, Source: European Union - EUR-Lex Last Accessed: 20/07/2023 Link: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32003H0361

1. its workforce
2. either sales or total assets



Company category	Staff headcount	Turnover	or	Balance sheet total
Medium-sized	< 250	≤ € 50 m		≤ € 43 m
Small	< 50	≤ € 10 m		≤ € 10 m
Micro	< 10	≤ € 2 m		≤ € 2 m

Figure 1: SME categorization table by EU criteria[8]

NACE classification

We have decided to consider the sectors of activities as defined by the NACE (Nomenclature des Activités Économiques dans la Communauté Européenne) classification system. The European Commission published a comprehensive list.[9] NACE, a European standard, serves as an industrial classification system. Its role is akin to the Standard Industrial Classification (SIC) and the North American Industry Classification System (NAICS), systems that categorize business activities.

1.4 – SMEs in Luxembourg

However, the term “SME” represents different realities, depending on the size of the company, which is an important determinant of the company’s ability to allocate resources to non-core activities.

The 2020 directory of Luxembourg companies published by STATEC[10] reveals that of the 37,807 companies in the country:

- 18,335 of them (48.5%) have just one employee,
- 11,063 have (29%) between 1 and 4 employees,
- 5,936 have (16%) between 5 and 19 employees,
- 1,440 entities (4%) hire between 20 and 49 people,
- 843 companies (2.5%) have between 50 and 249 employees.

[8] SME definition, Source: European Commission - Single Market Economy, Last Accessed: 20/07/2023 Link: https://single-market-economy.ec.europa.eu/smes/sme-definition_en

[9] List of NACE codes, Source: European Commission - Directorate-General for Competition, Last Accessed: 25/10/2023 Link: https://ec.europa.eu/competition/mergers/cases/index/nace_all.html

[10] Répertoire des Entreprises - 2020, Source: STATEC (Institut national de la statistique et des études économiques du Grand-Duché de Luxembourg) Last Accessed: 25/10/2023 Link: https://statistiques.public.lu/fr/publications/series/repertoire-entreprises/2020/repertoire-2020.html

The same directory presents the distribution of companies by their NACE Code.

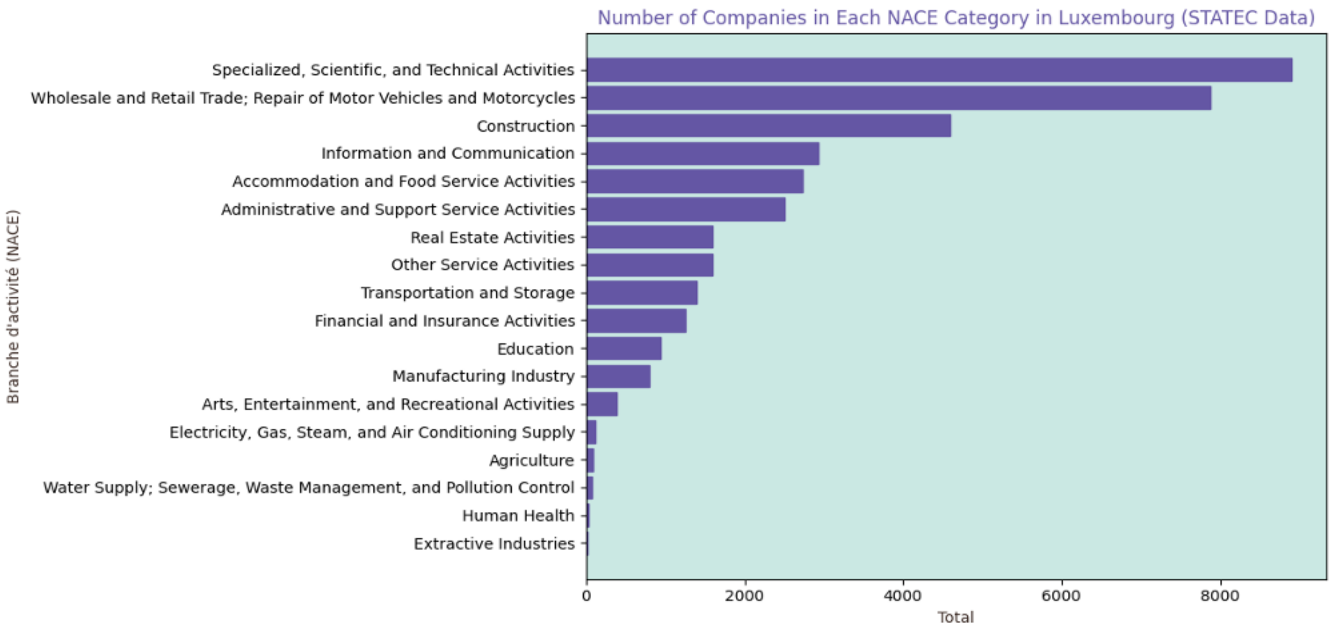


Figure 2: Number of companies in each NACE Category in Luxembourg based on STATEC Data 2020

2 – PEST matrix analysis

2.1 – Political & legal factors

The following analysis presents a detailed examination of the political and legal factors influencing cybersecurity landscape in Luxembourg for SMEs. We examine the centralized coordination led by the government, the country's integration of SMEs into cybersecurity strategies, and the economic implications of digital security as a national priority. Additionally, we address the influence of EU and local regulations on data protection and security, highlighting the roles of CNPD and CSSF in regulatory enforcement. Lastly, we look at the interplay between voluntary certification standards, like ISO/IEC 27001, and emerging EU mandates under the Cybersecurity Act, alongside Luxembourg's initiatives to facilitate compliance.

Centralized coordination mechanisms

The Luxembourg government has been proactive in fortifying its cybersecurity framework, notably through the establishment of the Cyber Security Board (CSB) in July 2011. Led by the Prime Minister, Xavier Bettel, the CSB has overseen the National Cybersecurity Strategies. The board has been complemented by a multi-disciplinary task force since 2014, which works in tandem to promote cybersecurity across sectors, with particular emphasis on SMEs. The country's comprehensive cyber defense strategy,[11] introduced in 2021, outlines Luxembourg's role within international organizations like NATO and the European Union, while also fostering collaboration with the private sector. The goal is to establish a resilient cybersecurity ecosystem that includes SMEs.

Cybersecurity as an economic incentive

In Luxembourg, cybersecurity transcends being a mere protective measure. It serves as the backbone of the country's economic strategy,[12] attracting business through a secure digital environment. The 2021 edition of the National Cybersecurity Strategy further spotlighted the role of SMEs, tying their cybersecurity needs to the activities of the Luxembourg House of Cybersecurity. Luxembourg, in line with broader European policy, is keenly on SMEs as pivotal agents for the digital transformation of the economy. The Ministry of the Economy' strategy, "Ons Wirtschaft vu muer",[13] rolled out in 2021, elaborates on this by outlining six essential pillars aimed at both economic development and digital transition.

Governmental pillars for digital adoption:

1. Accelerate digitization for societal benefit: Focus on rapid technological adoption for broad economic advantage.
2. Transition to a circular digital economy: Encourage digital solutions that support sustainable practices.
3. Develop resilient strategic value chains: Make supply chains robust and digitally secure.
4. Secure and reliable data economy transformation: Safeguard data transactions and storage.
5. Sustainable digital transition: Align digital practices with long-term sustainability goals.

[11] Presentation of Luxembourg's inaugural Cyber Defence Strategy, Source: Government of Luxembourg, Last Accessed 25/10/2023, Link: https://gouvernement.lu/en/actualites/toutes_actualites/communiques/2021/02-fevrier/12-bausch-strategie-cyberdefense.html

[12] National Cybersecurity Strategy IV, Source: High Commission for National Protection (HCPN), Luxembourg, Last Accessed 25/10/2023, Link: https://hcpn.gouvernement.lu/dam-assets/fr/publications/brochure-livre/strategie-nationale-cybersecurite-4/National-Cybersecurity-Strategy-IV.pdf

[13] Ons Wirtschaft vu muer - Feuille de route pour une économie compétitive et durable 2025, Source: Ministry of the Economy - Luxembourg, Last Accessed: 25/10/2023, Link: https://meco.gouvernement.lu/fr/publications/strategie/strategie-ons-wirtschaft.html

6. Favorable investment climate: Create a conducive environment for sustainable and competitive digital transformation.

Organizations like the Ministry of Small and Medium-Sized Enterprises, the Chamber of Crafts, and the Federation of Craftsmen have launched the "e-Handwierk" service under the broader "Pakt Pro Artisanat" program.[14] Other key governmental projects such as the "SME Packages – Digital" initiative,[15] for instance, expands the digital presence of SMEs focusing on digital marketing, management and electronic invoicing.

European regulations and local players

Among the key regulatory bodies, the National Commission for Data Protection (CNPD) is an essential player in shaping Luxembourg's cybersecurity landscape due to its responsibility of enforcing the General Data Protection Regulation (GDPR),[16] which is applicable to all businesses operating within the EU. Beyond the GDPR, the Network and Information Systems (NIS) directive[17] plays a significant role in setting cybersecurity requirements. The directive emphasizes the establishment of national Computer Security Incident Response Teams (CSIRTs) and the cultivation of a cybersecurity culture, particularly within essential service sectors. The initial NIS directive underwent revisions resulting in the NIS2,[18] expanding its scope to cover even small operators of critical infrastructure. This impacts SMEs, particularly those in industries like cloud computing and financial services, driving Luxembourg's public authorities to actively engage with SMEs to ensure compliance. Luxembourg's point of contact for NIS-related matters is the Institut Luxembourgeois de Régulation

[14] Le gouvernement et les organisations artisanales signent le "Pakt Pro Artisanat", Source: Fédération des Artisans (FDA) - Luxembourg, Last Accessed: 25/10/2023, Link: https://www.fda.lu/actualites/actualites/fda-actualites/le-gouvernement-et-les-organisations-artisanale-signen-le-pakt-pro-artisanat

[15] Les "SME-Packages": un soutien ciblé et efficace pour petites et moyennes entreprises, Source: Government of Luxembourg, Last Accessed: 25/10/2023, Link: https://gouvernement.lu/fr/actualites/toutes_actualites/communiques/2022/09-septembre/29-delles-sme.html

[16] General Data Protection Regulation, Source: EUR-Lex (Official Journal of the European Union), Last Accessed: 25/10/2023, Link: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[17] The NIS2 Directive: A high common level of cybersecurity in the EU, Source: European Parliament – Think Tank, Last Accessed: 25/10/2023 Link: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333

[18] Proposal for directive on measures for high common level of cybersecurity across the Union, Source: European Commission, Last Accessed: 25/10/2023, Link: https://digital-strategy.ec.europa.eu/fr/node/433

(ILR). Sector-specific regulations in Luxembourg exert significant influence on the market's key players and their service providers. This is especially evident in the banking and financial sectors, given their prominence in the overall economy. The Commission de Surveillance du Secteur Financier (CSSF) play a critical role in this landscape, it is particularly involved in the enforcement of the Digital Operational Resilience Act (DORA),[19] which entered into force in January 2023. Finding the balance between regulations and day to day operation is a hard challenge which could become a burden as highlighted in PwC Annual Global CEO Survey's key findings for Luxembourg[20] in terms of over-regulation which could be an issue both for companies and the competitiveness of the country compared to similar financial hubs such as the United Kingdom or Singapore.

Certification vs. regulation: Market distinction and the EU cybersecurity shift

Certification, often a voluntary process except when required by law or regulation, formally acknowledges compliance with predefined standards, such as the ISO/IEC 27001[21] in cybersecurity, which is typically pursued by entities with advanced cybersecurity practices. According to the 2021 ISO study on country-specific certifications,[22] Luxembourg had 43 entities certified in ISO 27001, a significant increase on the 10 entities recorded up to 2015,[23] but still very limited in relation to the total number of companies. The introduction of the Cybersecurity Act (CSA),[24] which came into force on 27 June 2019, represents a significant shift in the landscape of cybersecurity within the EU. It aims to create a unified framework for cybersecurity certification across Europe, thereby eliminating the fragmentation of regulations and

[19] Digital finance: Council adopts Digital Operational Resilience Act, Source: Council of the European Union, Last Accessed: 25/10/2023, Link: https://www.consilium.europa.eu/en/press/press-releases/2022/11/28/digital-finance-council-adopts-digital-operational-resilience-act/

[20] The cloud of over-regulation that shades CEOs' optimism, Source: PwC Luxembourg, Last Accessed: 08/11/2023, Link: https://blog.pwc.lu/over-regulation-a-big-concern-to-luxembourg-ceos/

[21] ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection, Source: ISO, Last Accessed: 06/11/2023, Link: https://www.iso.org/standard/27001

[22] ISO Survey of certifications to management system standards - Full results, Source: ISO, Last Accessed: 06/11/2023, Link: https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1

[23] The ISO Survey of Management System Standard Certifications (2006-2015), Source: ISO, Last Accessed: 06/11/2023, Link: https://www.iso.org/files/live/sites/isoorg/files/standards/conformity_assessment/certification/doc/Survey-data/iso_27001_iso_survey2015.xls

[24] The EU Cybersecurity Act, Source: European Commission, Last Accessed: 06/11/2023, Link: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

standards among Member States. The CSA introduces different levels of assurance (basic, substantial, high) to categorize the risk levels of ICT products, services, and processes, making it easier for organizations to align their cybersecurity measures with the level of risk they face. Certifications obtained under the CSA framework are recognized across all EU Member States, simplifying the certification process for companies operating in multiple countries. While certifications have been largely voluntary, the CSA indicates a future where certain certifications may become mandatory, especially for critical infrastructure and services. In Luxembourg, the CORAL Project[25] aims to simplify the CSA certification process at the basic level, making it more accessible for ICT market players and especially SMEs developing ICT products, services, or processes, acting in any sector.

2.2 – Economic factors

In this section, we explore economic factors impacting cybersecurity among Luxembourg's SMEs. We assess ENISA's findings on SMEs' financial hurdles in implementing cyber defenses and examine the digital adoption rates reported by the OECD, noting their effect on SMEs' cyber vulnerability. We also highlight Luxembourg's investment in technology sectors—space, fintech, healthtech—and the corresponding cybersecurity risks. Government efforts through STARTUP LUXEMBOURG to nurture these sectors are discussed, emphasizing the cybersecurity implications in an evolving digital-focused startup landscape.

Cybersecurity as a perceived financial burden

The issue of cybersecurity is often perceived through the lens of financial constraints by Luxembourg's SMEs, according to findings from ENISA's report on SMEs. This view is compounded by several factors, from their limited ability to gauge the risks and consequences of cybersecurity threats to their lack of negotiation power in service level agreements.[26] The limited bargaining power of SMEs in contract negotiations, owing to their small size, prevents them from securing favorable terms in service level agreements. This disadvantage prevents them from accessing cost-effective cybersecurity solutions tailored to their specific needs. Consequently, SMEs face higher costs, inadequate protection, and a competitive disadvantage. The

[25] CORAL-Project A CSA compliant self-assessment and basic level certification framework, Source: Coral Project, Last Accessed: 06/11/2023, Link: https://coral-project.org/

[26] Cybersecurity for SMEs - Challenges and Recommendations, Source: ENISA, Last Accessed: 25/10/2023, Link: https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes

Telindus 2022 Benelux report[27] highlights that 1 out of 5 companies have increased its budget in the past year, however this trend is mostly led by efforts within large companies. The cybersecurity budget discussion, as unveiled by a PwC study on Chief Information Security Officer (CISO) and Data Protection Officer (DPO) roles[28] in various Luxembourg companies, reveals a trend that may not fully capture the entire reality. Among the findings, 57% of CISOs reported not having a budget, and 45% expressed dissatisfaction considering their budget insufficient.

Consequences of digitization on cybersecurity

The landscape of digital tool adoption for revenue generation among SMEs presents a distinct two-tiered scenario, as illuminated by insights from the OECD's "SME and Entrepreneurship Outlook 2021".[29] While 58.8% of companies actively leverage social media platforms for promotional activities, a mere 25.1% harness the potential of cloud services, and a scant 11.8% engage in e-commerce endeavors. Notably, this digital presence, or lack thereof, carries intrinsic implications, as highlighted in the ENISA Threat report 2022[30] as approximately 82% of breaches involve a human element, with as many as 60% of breaches in Europe, the Middle East, and Africa incorporating an element of social engineering. As Luxembourg's SME sector accelerates its digital transformation, a concomitant rise in cybersecurity challenges manifests. The push towards digitization, while fostering economic growth and efficiency, has inadvertently expanded the cyber-attack surface. The introduction of digital tools amplifies the complexity of security landscapes, especially as SMEs adopt remote work setups, IoT devices, and AI-driven processes. While the advent of digital tools has dramatically boosted productivity, it has simultaneously made businesses susceptible to a myriad of cyber threats. As demonstrated by the Threat Observatory Platform phishing attacks, ransomware, and data breaches. Without

[27] Telindus 2022 research report of the impact of cybersecurity on companies in the Benelux, Source: Telindus, Last Accessed: 02/11/2023, Link: https://cybersecurity.proximus.be/research-report-2022/results

[28] Out of the Shadows: CISO and DPO in the Spotlight 2022, Source: PwC Luxembourg, Last Accessed: 08/11/2023, Link: https://www.pwc.lu/en/advisory/digital-tech-impact/cyber-security/out-of-the-shadows-ciso-and-dpo-in-the-spotlight-2022.html

[29] OECD SME and Entrepreneurship Outlook 2021, Source: OECD, Last Accessed: 17/04/2023, Link: https://www.oecd.org/publications/oecd-sme-and-entrepreneurship-outlook-2021-97a5bbfe-en.htm

[30] Volatile Geopolitics Shake the Trends of the 2022 Cybersecurity Threat Landscape, Source: ENISA, Last Accessed: 25/10/2023, Link: https://www.enisa.europa.eu/news/volatile-geopolitics-shake-the-trends-of-the-2022-cybersecurity-threat-landscape

rigorous cybersecurity practices in place, the data and digital assets of SMEs stand vulnerable. For many SMEs in Luxembourg, especially those lacking resources or expertise, this represents a pressing concern.

A growing economy with a focus on cutting-edge technologies

Luxembourg is strategically focusing on next-gen technologies, evident in the flourishing sectors of space, fintech, and healthtech. This momentum is the result of collaboration between the government, academic institutions, research centers and leading incubators. Luxembourg's growing emphasis on space resources and technology brings about unique cybersecurity concerns. This sector which already boasts around 50 companies, welcomes the European Space Resources Innovation Centre (ESRIC),[31] and has a dedicated public agency tied to the Ministry of Economy.[32] It alone comprises more than 20 start-ups, making up 40% of the industry.

The Luxembourg economy has a significant share of start-ups specializing in fintech, or financial technologies, with over 200 players identified by the LHoFT Foundation's 2022 mapping study.[33] The government is focusing a large part of its efforts on this sector, particularly on blockchain technologies, a promising tool not only for digital transactions but also for enhancing cybersecurity measures. However, given that fintech startups frequently manage substantial volumes of sensitive financial data, they become prime targets for cyber-attacks. The increasing digitization of health records, medical processes, and patient data means that these startups might be lucrative targets for cyber attackers. Luxinnovation highlighted in 2020 that the sector has 136 companies with an increasing number of companies with a digital focus.[34] Unauthorized access to sensitive health information, disruption of medical services, or tampering with medical equipment can have dire consequences, both legally and in terms of patient safety.

The Luxembourg government is keen to support the growth of these players to establish the country as a technological hub. The STARTUP LUXEMBOURG

[31] European Space Resources Innovation Centre, Source: ESRIc, Last Accessed: 25/10/2023, Link: https://www.esric.lu/

[32] Business Sector - Space, Source: Luxembourg Trade & Invest, Last Accessed: 25/10/2023, Link: https://www.tradeandinvest.lu/business-sector/space/

[33] The Luxembourg Fintech Map, Source: LHoFT, Last Accessed: 25/10/2023, Link: https://lhoft.com/en/insights/the-luxembourg-fintech-map/

[34] Key figures about the HealthTech private sector in Luxembourg (2020), Source: Luxinnovation, Last Accessed: 25/10/2023, Link: https://www.luxinnovation.lu/healthtech-mapping/

initiative,[35] driven by the Ministry of Economy via its agency Luxinnovation, focuses on supporting these entities by highlighting local actions and businesses. According to the national ecosystem mapping of start-ups in 2021,[36] Luxembourg has over 500 such companies, primarily in the areas listed below.

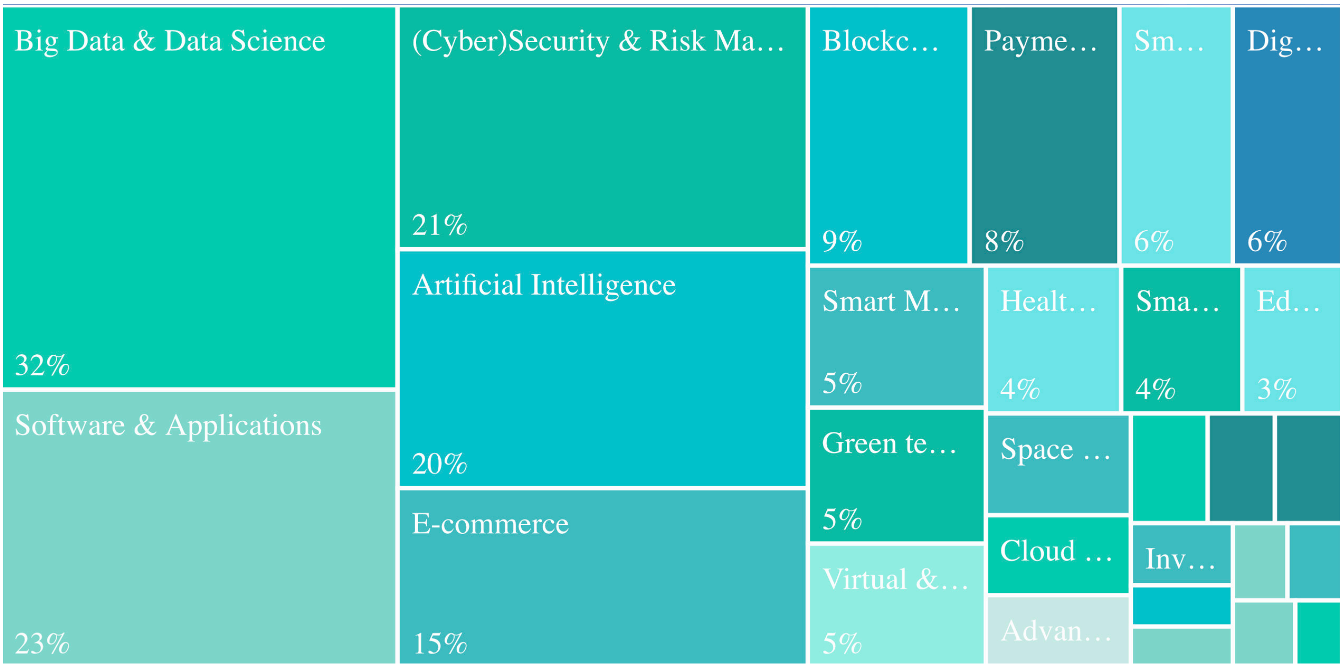


Figure 3: Treemap diagram of startups categorized by key technologies according to Luxinnovation's 2021 data

2.3 – Social factors

This section examines the social factors influencing cybersecurity among Luxembourg's SMEs. It considers the diverse and cross-border nature of the workforce and its implications for the management of cybersecurity protocols. The analysis also evaluates the uneven distribution of digital skills across various demographics, identifying potential vulnerabilities within cybersecurity frameworks. Furthermore, the current impact of the global shortage of cybersecurity professionals on Luxembourg's market is explored, with particular attention to its effects on the availability of expertise for SMEs. Finally, the extent of cybercrime experiences within SMEs and the prevailing cybersecurity awareness among employees are examined, drawing insights into the preparedness and responsiveness of these businesses to cyber threats.

[35] Startup Luxembourg, Source: Startup Luxembourg, Last Accessed: 25/10/2023, Link: https://www.startupluxembourg.com/

[36] Luxembourg startup ecosystem, Source: Luxinnovation, Last Accessed: 17/05/2023 https://app.powerbi.com/view?r=eyJrIjoiMTFjNDMwYTUtMDZhZS00ODAxLWExY2EtOTI5ZTZlZDlhZWNjIiwidCI6ImRiNGE4Mjc4LWE3NjMtNGIzYS1hZjY3LWQ2MzE2NDVmYTRlMCIsImMiOjl9

The human factor in a cosmopolitan, cross-border society

According to 2021 Eurostat data, Luxembourg had 36,751 SMEs, constituting 99.5% of all businesses and employing 202,871 individuals or 66.0% of the active workforce.[37] A key aspect of Luxembourg's economy is the large foreign resident and cross-border workforce. According to 2022 IGSS data,[38] out of 475,860 employees, only 138,540 are Luxembourgers, making up 29.10% of the active population. The most represented nationalities in the Luxembourgish workforce include the French (24.81%), Portuguese (11.99%), Belgians (9.95%), and Germans (9.62%). However, the majority of these workers, 63% of the active population, reside in their home countries. This diversity adds layers of complexity to cybersecurity protocols. One issue is that cybersecurity awareness materials need to be translated into multiple languages spoken and understood by the workforce. This is not a trivial task and adds complexity to company-wide security measures. The human factor remains the weakest security link, susceptible to various types of attacks such as phishing and spear phishing. In its 2021 SME Cybersecurity Guide,[39] the European Union Agency for Cybersecurity (ENISA) reveals that many companies have permitted the use of personal digital devices for work, a trend exacerbated by the COVID-19 pandemic. This practice expands the attack surface and complicates the task of maintaining uniform security standards across the organization. The ENISA also underscored a significant concern: regulatory inconsistencies in cybersecurity directives translation among EU member states. This lack of uniformity complicates compliance for SMEs operating across multiple EU countries or having employees working remotely from their homes located in a neighboring country of Luxembourg.

[37] SME Performance Review 2021/2022 - Luxembourg country sheet, Source: European Commission, Last Accessed: 25/10/2023, Link: https://ec.europa.eu/docsroom/documents/50696

[38] Résidence et nationalité des salariés qui travaillent au Luxembourg, Source: IGSS, Last Accessed: 26/10/2023, Link: https://app.powerbi.com/view?r=eyJrIjoiYTQ0ZWQ1NTc tNjI3MC00ZTQzLWJiNWQtYzRiNzA4ZTk4MDg1IiwidCI6ImNmZjViYTQyLWNlZDktNDA2NS04MjI2LTBjODI4YjM4M2RjNSIsImMiOjl9

[39] Cybersecurity for SMEs - Challenges and Recommendations, Source: ENISA, Last Accessed: 26/10/2023, Link: https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes

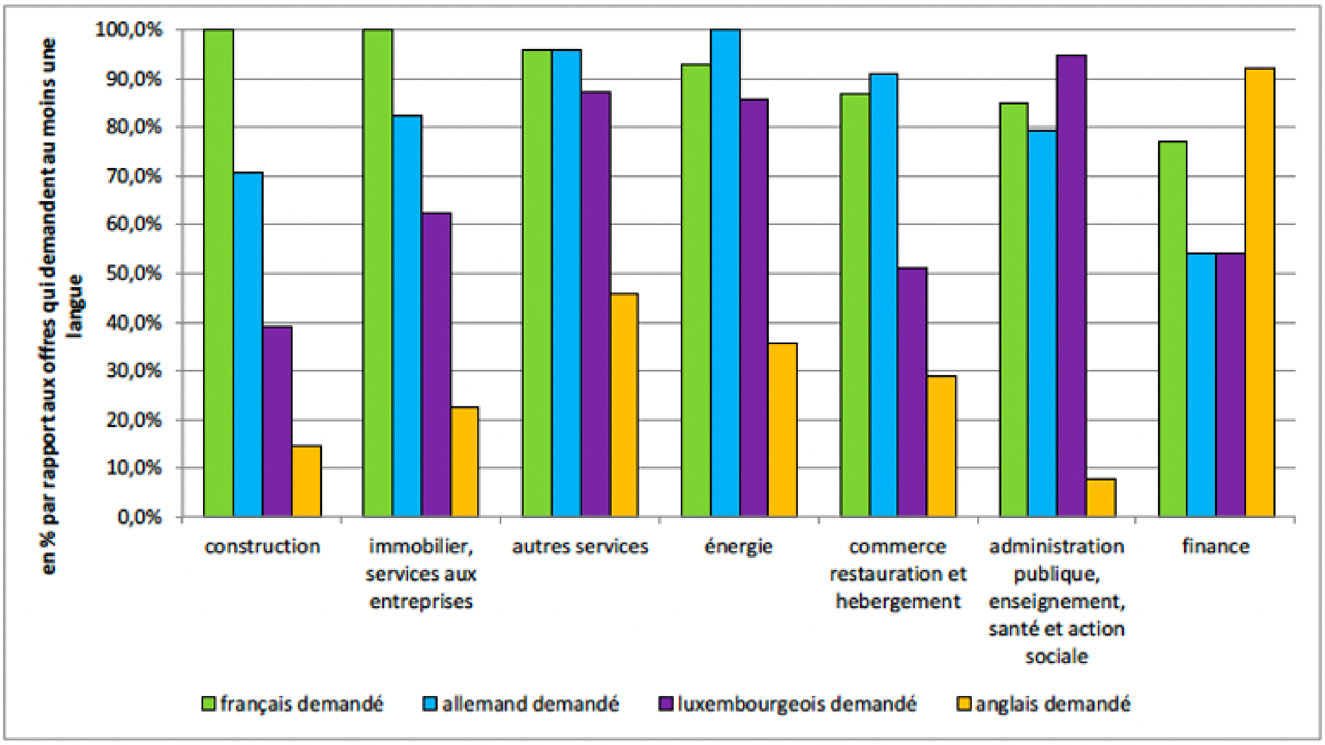


Figure 4: Distribution of industry-required languages as a percentage compared to job offers that necessitated at least one language in 2019[40]

Uneven distribution of digital skills

The 2021 Eurostat study on basic digital knowledge reveals that Luxembourg ranks tenth among European Union members, with 64% of its population possessing fundamental digital skills.[41] However, this average conceals significant disparities related to age and educational levels. STATEC's 2020 study on ICT usage highlights a noticeable gap in the utilization of online public services between highly-educated individuals and those with lower educational attainment.[42] Additionally, Luxembourg boasts one of the highest proportions of ICT specialists in Europe, nearly 7% of the

[40] L'emploi frontaliers par secteurs d'activité, Source: IBA-OIE, Last Accessed: 26/10/2023, Link: https://www.iba-oie.eu/fr/themes/mobilite-des-frontaliers/luxembourg/lemploi-frontaliers-par-secteurs-dactivite

[41] Individuals' level of digital skills (from 2021 onwards) Eurostat Data Browser - Custom Table, Source: Eurostat, Last Accessed: 26/10/2023, Link: https://ec.europa.eu/eurostat/databrowser/view/ISOC_SK_DSKL_I21__custom_2397093/bookmark/table?lang=en&bookmarkId=dc481686-c938-4e07-b03c-8e039f532857

[42] N° 22/2020 - L'administration en ligne au Grand-Duché : Guichet.lu adopté par les internautes, Source: STATEC (Institut national de la statistique et des études économiques du Grand-Duché de Luxembourg), Last Accessed: 26/10/2023, Link: https://statistiques.public.lu/fr/publications/series/regards/2020/regards-22-20.html

total workforce, trailing only Sweden and Finland.[43] While Luxembourg has a relatively high overall level of digital competence, the existing educational and age-related disparities reveal a complex landscape. Individuals with higher education are more likely to utilize online public services, revealing a divide in the practical application of digital literacy.

Luxembourg's position amidst the global cybersecurity skills shortage

All over the world, the shortage of IT and cybersecurity professionals is recognized and is getting worse. This alarming shortage, highlighted by the World Economic Forum, reflects an ever-widening gap: while cyber threats are proliferating, the expertise needed to deal with them is not up to scratch.[44] Despite better positioning than many nations,[45] Luxembourg isn't exempt from the challenges posed by the global cybersecurity talent crunch. The country's dynamic financial sector, renowned for its competitive edge, often attracts the lion's share of top IT and cybersecurity talent. Given the financial sector's complex security requirements and attractive remuneration packages, it's no surprise that many skilled professionals are attracted to the sector. However, this could leave the SME sector in the lurch, potentially lacking the cybersecurity expertise essential to its protection.

Cybercrime impact and response in Luxembourg SMEs

According to the Flash Eurobarometer on SMEs and Cybercrime,[46] based on 2021 data from Luxembourg, a majority of business leaders are highly concerned about various cyber risks. The same study reveals that 26% of companies have faced at least one of eight types of cybercrime incidents in the past year—2 percentage points above the European average. In 33% of these instances, the incidents resulted in significant operational challenges, such as the inability of employees to work, increased workload, and discouragement to carry out planned activities. However,

[43] ICT specialists in employment, Source: Eurostat, Last Accessed: 26/10/2023, Link: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_specialists_in_employment

[44] Can closing the cybersecurity skills gap change the world?, Source: World Economic Forum, Last Accessed: 26/10/2023, Link: https://www.weforum.org/agenda/2022/03/closing-the-cybersecurity-skills-gap/

[45] ICT specialists in employment, Source: Eurostat, Last Accessed: 26/10/2023, Link: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_specialists_in_employment

[46] SMEs and Cybercrime - Eurobarometer Survey, Source: European Union, Last Accessed: 26/10/2023, Link: https://europa.eu/eurobarometer/surveys/detail/2280

regarding employee awareness and training, this study reveals that most business leaders believe their employees are well or very well informed about cybersecurity risks, with 43% and 28% respectively thinking this way. Yet, 79% of these companies have not provided their employees with training on this subject in the past year. Based on a European Commission study, Luxembourg ranks 21st in terms of companies that raise awareness among employees about their ICT security obligations.[47] Furthermore, only about half of the companies possess some form of cybersecurity policy documentation.[48] This situation indicates a potential lack of preparation and possibly a disparity between the perceptions of business leaders and the actual level of cybersecurity preparedness within their organizations.

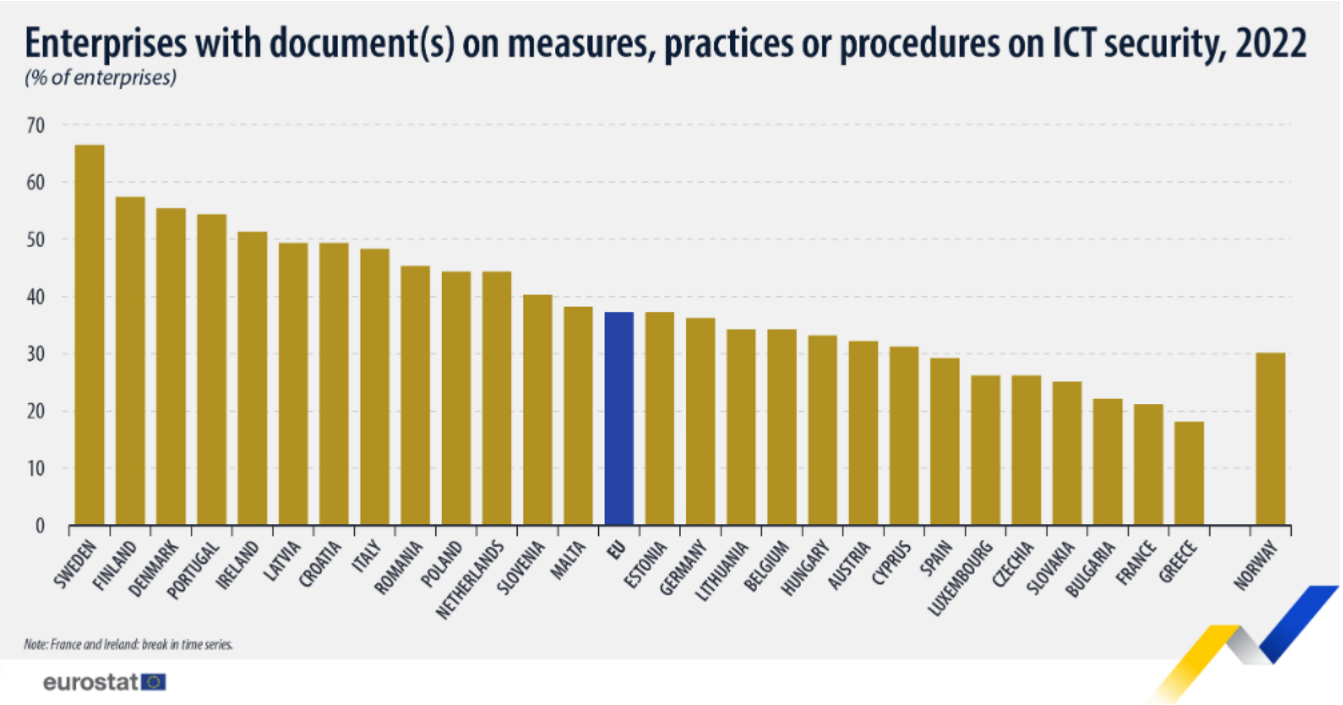


Figure 5: Luxembourg ranks 22nd in terms of the percentage of companies with documents on ICT security measures, practices or procedures.

[47] Enterprises making persons employed aware of their obligations in ICT security related issues by any measure, 2019 (% enterprises), Source: Eurostat Statistics Explained, Last Accessed: 26/10/2023, Link: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=File:Enterprises_making_persons_employed_aware_of_their_obligations_in_ICT_security_related_issues_by_any_measure,2019(%25_enterprises).png

[48] Enterprises with document(s) on measures, practices or procedures on ICT security, 2019 (% enterprises), Source: Eurostat Statistics Explained, Last Accessed: 26/10/2023, Link: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=File:Enterprises_with_document(s)_on_measures,_practices_or_procedures_on_ICT_security,2019(%25_enterprises).png

2.4 – Technological factors

This segment of the PEST analysis focuses on technological factors impacting Luxembourg's SMEs in cybersecurity. We analyze the disparity in digital integration rates between large enterprises and SMEs, despite Luxembourg's high DESI ranking. The focus is on the need for advanced cybersecurity measures to address supply chain vulnerabilities and the growing sophistication of AI-based cyber threats. The potential of AI, particularly Large Language Models (LLM), in enhancing SMEs' cybersecurity posture is also examined. This assessment provides a technical snapshot of the challenges and opportunities in Luxembourg's digital transformation journey for SMEs.

Luxembourg's two-speed technological integration: a road to progress and a set of challenges

According to the 2022 Digital Economy and Society Index (DESI),[49] Luxembourg ranks 8th among the 27 European Union countries. The country is on a good path toward fulfilling the goals set out in the "Action Programme: The Path Forward for the Digital Decade"[50] which includes:

1. Equipping the population with digital skills,
2. Having secure and sustainable digital infrastructures,
3. Digital transformation of businesses, and
4. Digitization of public services.

However, with an annual growth rate of 6%, Luxembourg is lagging behind countries with similar DESI scores. Luxembourg's weak points in comparison to the EU average include technological integration and connectivity, characterized by low uptake of 1 Gbps internet, limited 5G coverage, and high broadband costs. Additionally, the country lags in e-commerce, with only 9% of SMEs selling online (against the EU average of 18%) and a decrease in cross-border online sales by SMEs.

[49] Luxembourg in the Digital Economy and Society Index, Source: European Commission, Last Accessed: 26/10/2023, Link: https://digital-strategy.ec.europa.eu/en/policies/desi-luxembourg

[50] Europe's Digital Decade, Source: European Commission, Last Accessed: 26/10/2023, Link: https://digital-strategy.ec.europa.eu/fr/policies/europes-digital-decade

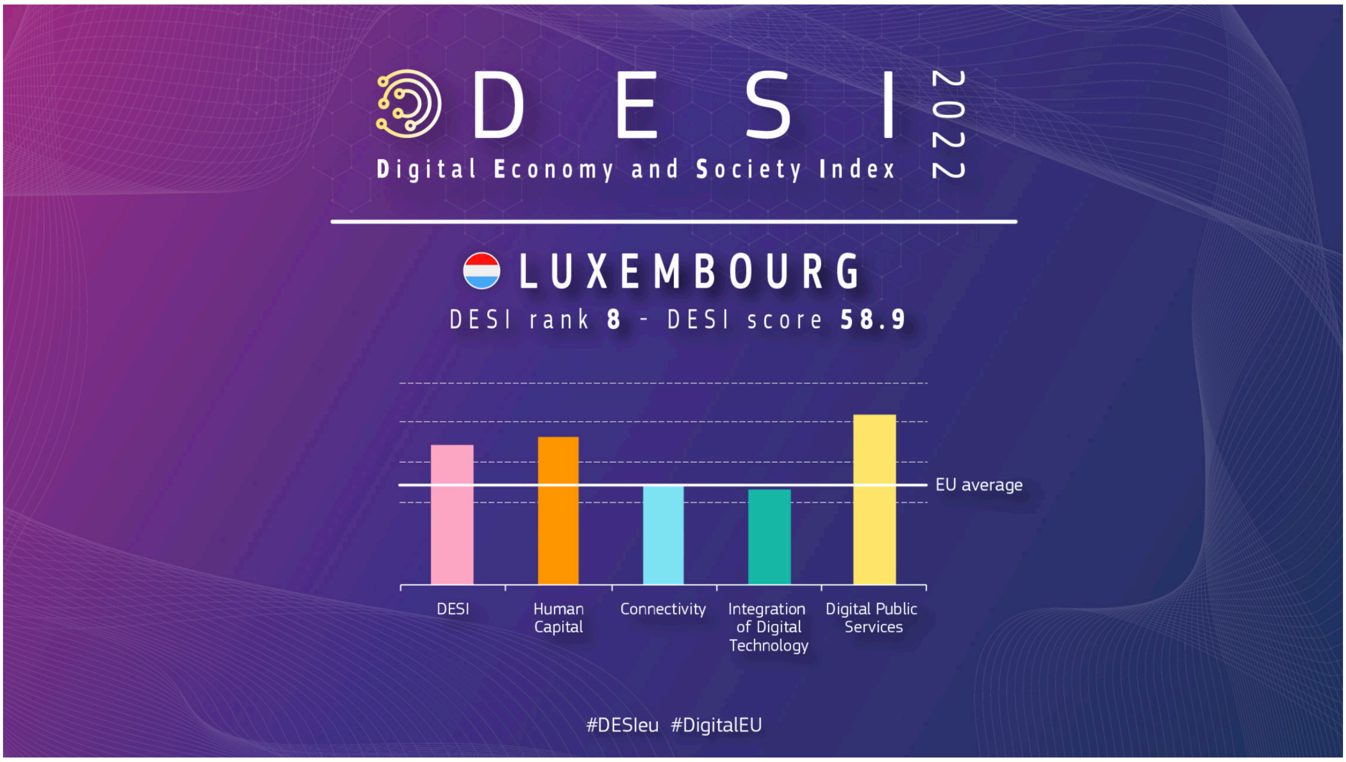


Figure 6: Digital Economy and Society Index (DESI) 2022 country report

Although Luxembourg enjoys a ranking of 15th in the 2021 Digital Intensity Index,[51] this statistic masks underlying disparities. Advanced actors, especially large enterprises, tend to skew the national average upward, leaving behind a significant percentage of SMEs that employ rudimentary technological tools in their day-to-day operations. This presents a dual-speed technological environment, where state-level initiatives are racing ahead, but the SME sector is not keeping pace, thereby widening the technology gap. Bridging this gap is crucial for ensuring that the country's aspirations translate into tangible progress across all sectors of the economy.

Supply chain vulnerabilities

The complexity of supply chains and limited visibility into the cybersecurity of numerous partners and suppliers exacerbate these risks, highlighting the need for robust cyber security strategies among SMEs. While many SMEs lack the technical and legal skills to manage their cybersecurity, they often rely on service providers for implementing solutions and maintaining systems. Vulnerabilities,[52] such as the flaw in Microsoft Exchange's email service, often go untreated for months or even years after being disclosed. The cybersecurity threat landscape in Luxembourg has changed

[51] How digitalised are the EU's enterprises?, Source: Eurostat, Last Accessed: 26/10/2023, Link: https://ec.europa.eu/eurostat/web/products-eurostat-news/-/ddn-20220826-1

[52] Common Vulnerabilities and Exposures (CVE), Source: MITRE Corporation, Last Accessed: 26/10/2023, Link: https://cve.mitre.org/

dramatically in recent years, as noted by Alexandre Dulaunoy, security researcher and head of CIRCL. While phishing attempts have historically been a dominant attack vector, publicly exposed services have emerged as the primary entry point for most impactful incidents targeting SMEs in 2023. This encompasses a range of exposed public vulnerable services, including VPN gateways, mail servers, and even security devices. Evidence of this trend is seen in the over 15,000 notifications issued by CIRCL concerning such vulnerable services in just a single year. The merging of traditional ICT and OT systems, like ICS and SCADA, has heightened security risks. Originally isolated OT systems from the 1990s are now part of modern IP networks, leading to new vulnerabilities.

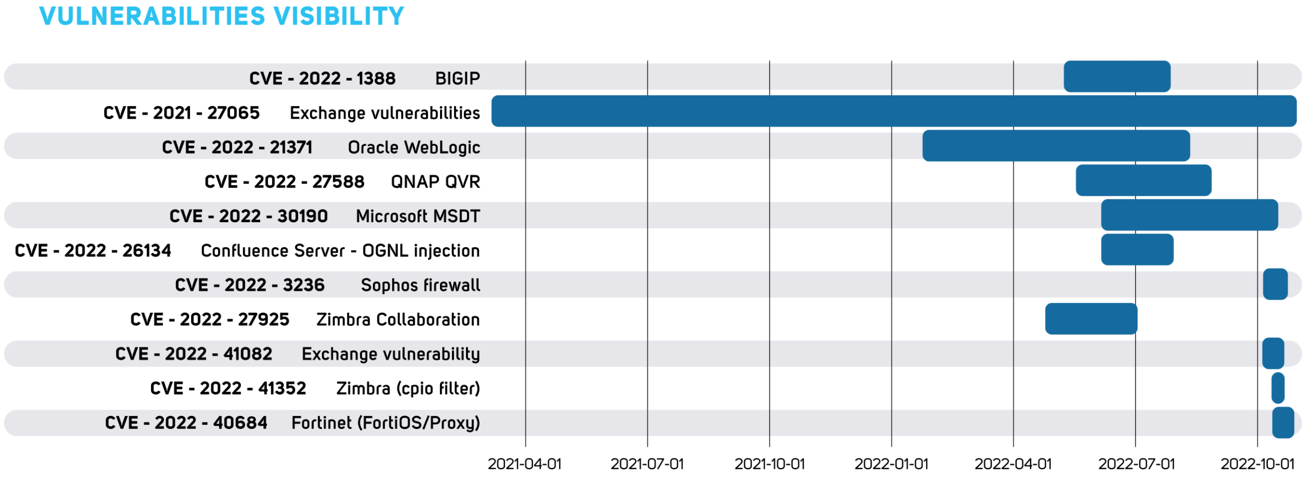


Figure 7: Table showing CVE incidents in Luxembourg since their publication in the MITRE directory[53]

Leveraging AI for adaptive cybersecurity solutions

The rapidly evolving digital landscape and the nuanced cybersecurity challenges of SMEs highlight an unmet need for adaptive, AI-driven solutions. The open-source availability of advanced Large Language Models (LLMs), such as ChatGPT,[54] presents a transformative opportunity. LLMs can not only assist SMEs in finding answers to pressing cybersecurity questions but can also aid in effortlessly drafting comprehensive security plans, essentially bridging the gap in basic cybersecurity consulting. Startups and research programs, both public and private, stand at the forefront of this revolution. They are well-equipped to develop AI-powered tools

[53] CYBERSECURITY Threat Landscape Luxembourg, 2021-22, Source: Luxembourg House of Cybersecurity, Last Accessed: 02/11/2023, Link: https://lhc.lu/news/new-cybersecurity-threat-landscape-luxembourg-221-22

[54] ChatGPT, Source: OpenAI Last Accessed: 26/10/2023, Link: https://chat.openai.com/

tailored to the multifaceted nature of SME environments.

AI-driven threats: navigating the evolving cybersecurity landscape for SMEs

The advent of AI technologies, notably LLMs and neural net tools, introduces heightened cybersecurity challenges for SMEs. Jean-Louis Huynen, security researcher at CIRCL, highlights the emergence of intricate social engineering attacks, facilitated by AI advancements. Examples include bots fostering long-term trust relationships or conducting direct phone conversations, posing genuine threats. These attacks manifest in forms like spear-phishing, basic impersonations with craftily penned requests for wire transfers, or sophisticated impersonations using spoofed emails and counterfeit business discussions. Additionally, the proliferation of computer-generated content, from voice mimicry to deep-fakes, further complicates the digital realm. The onset of Virtual and Augmented Reality (VR & AR) exacerbates the difficulty in discerning online content's authenticity. Determining a URL's intent becomes akin to a treacherous journey, challenging users to differentiate between benign and malicious content. Though Root Cause Analysis (RCA) is intricate, observation and reporting tools provide a semblance of a safeguard.

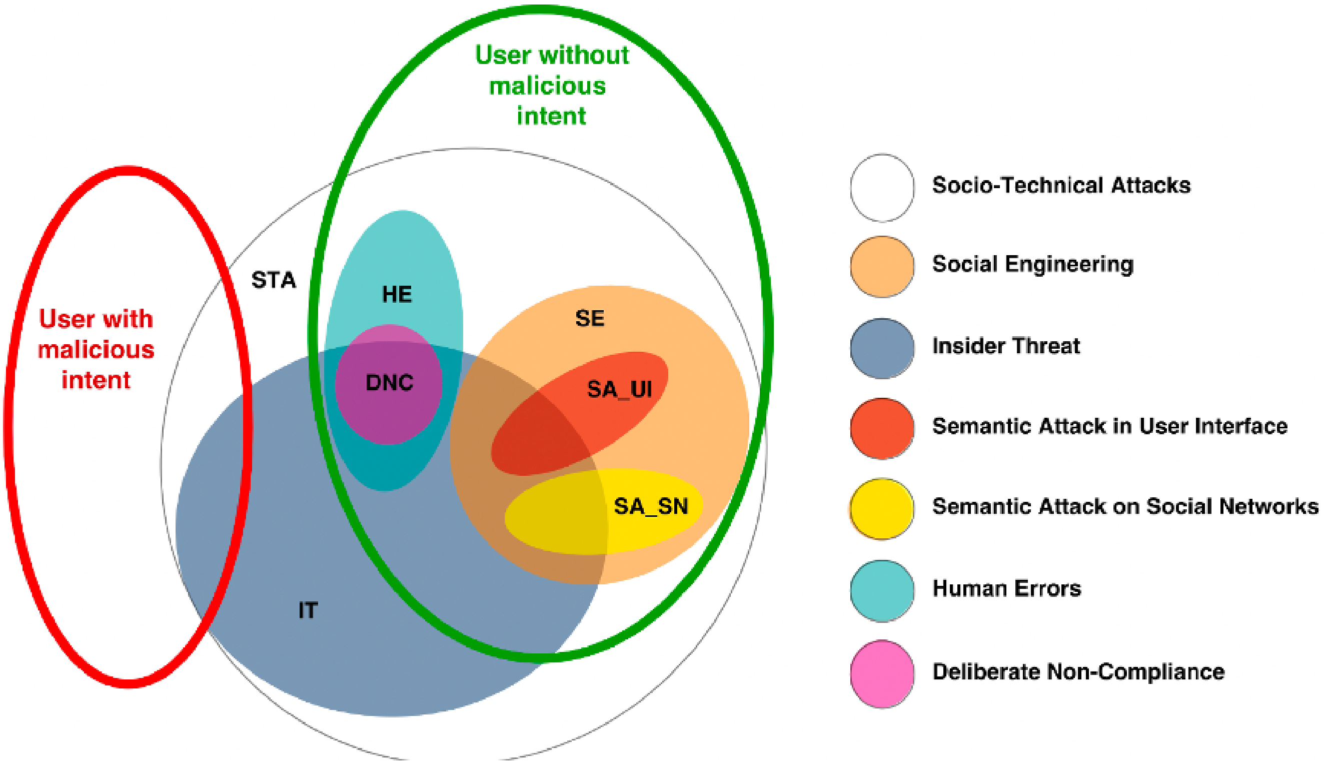

User without malicious intent
User with malicious intent
STA
HE
DNC
SE
SA_UI
SA_SN
IT
Socio-Technical Attacks
Social Engineering
Insider Threat
Semantic Attack in User Interface
Semantic Attack on Social Networks
Human Errors
Deliberate Non-Compliance

Figure 8: Socio-technical attacks representation from the 'Human using technology, monkeys living at the edge of chaos' presentation by Jean-Louis Huynen

2.5 – Research hypothesis for the identification of information gaps

The PEST matrix analysis revealed key insights and identified information gaps, which we have translated into research hypotheses. These hypotheses, based on each element of the PEST framework, will guide the creation of survey and focus group questions for the next stage of our study involving Luxembourg SMEs.

Political & legal factors

- SMEs are too diverse a type of actor to be treated in a one-size-fits-all way.
- Certificates and statuses are only attractive if they represent a legal requirement or a decisive competitive advantage for SMEs.

Economic factors

- The price of cybersecurity services is a barrier to the adoption of cybersecurity measures.
- The extensive use of new technologies by certain companies makes these entities more exposed to cyber threats.

Social factors

- Employees' digital practices could become new risks for SMEs.
- A portion of SMEs measure their cyber risk based on their leaders' understanding.
- The level of SMEs in terms of protection against cyber threats depends on their ability to find experts in the field.

Technological factors

- The integration of technologies in the private sector is a driver for the development of a cybersecurity culture.
- The cybersecurity services available are not tailored to the needs of SMEs.
- Only automated solutions provided by public actors can have significant consequences on the cybersecurity level of SMEs.

In the upcoming chapter, we present the results of our survey, which was designed in alignment with the criteria and insights highlighted in this analysis. This survey, combined with group discussions, aims to explore and validate the research hypotheses derived from the PEST framework in the context of the Luxembourg SME sector.

3 – Survey question formulation and analysis of responses

To provide insights in answering our research hypothesis we formulated a series of questions which we distributed to Luxembourg SME using an internal online tool, known as Fit4Cybersecurity.[55] The survey was built by the LHC – NC3 team, reviewed by representatives of professional organisations, and promoted with their support via digital channels. The support of these key players allowed to share this content to a large audience of companies. The full set of questions and answers is available on GitHub.[56] The content below presents the survey results for each question, along with some additional contextual information about the campaign.

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

- Total: 143
- Finished: 101 – 70.6%
- In progress: 38 – 26.6%
- Under review: 4 – 2.8%

The survey also reveals the language preferences of the respondents:

- French: 67 – 66%
- English: 22 – 22%
- German: 12 – 12%

The dataset of questions is organized into several categories as shown below, with each section including only the fully completed responses (101 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. The following sections focus on cybersecurity practices, in order to obtain information relevant to our research hypotheses.

Socio-economic data

In the socio-economic data section, we gathered detailed information about the respondents' positions, the sizes of their organizations, and sectors of activity, as

[55] SurveySMEDemand branch of the Fit4Cybersecurity GitHub repository, Source: GitHub Last Accessed: 06/11/2023, Link: https://github.com/NC3-LU/Fit4Cybersecurity/tree/surveySMEDemand

[56] Questions available as JSON file on the SurveySMEDemand branch of the Fit4Cybersecurity GitHub repository, Source: GitHub Last Accessed: 07/11/2023, Link: https://github.com/NC3-LU/Fit4Cybersecurity/blob/surveySMEDemand/data/surveySMEDemand/questions.json

classified by NACE codes, to enhance our understanding of their representation within Luxembourg's SME sector. A significant portion of the respondents (47.5%) were CEOs or business owners, followed by 11.9% in unclassified job titles, and 10.9% holding other director roles. The company sizes showed a nearly equal distribution across three categories: fewer than 250, fewer than 50, and fewer than 10 employees. Notably, only 7% of responses came from single-employee companies. Geographically, most respondents' companies were located in the canton of Luxembourg, Esch-sur-Alzette, and Capellen, the country's largest business hubs. Regarding sectors, one-fourth operated in the Construction sector (NACE Code F), followed by 17% in Other Services Activities (NACE Code S), and 12% in Information and Communication (NACE Code J). While a majority of NACE codes were represented in the dataset, some, like Accommodation and Food Service Activities (NACE Code I), Activities of Households as Employers (NACE Code T), and Arts, Entertainment, and Recreation (NACE Code R), were less prominent, each accounting for just 1% of responses.

Q1 – *What is your position within the company?*

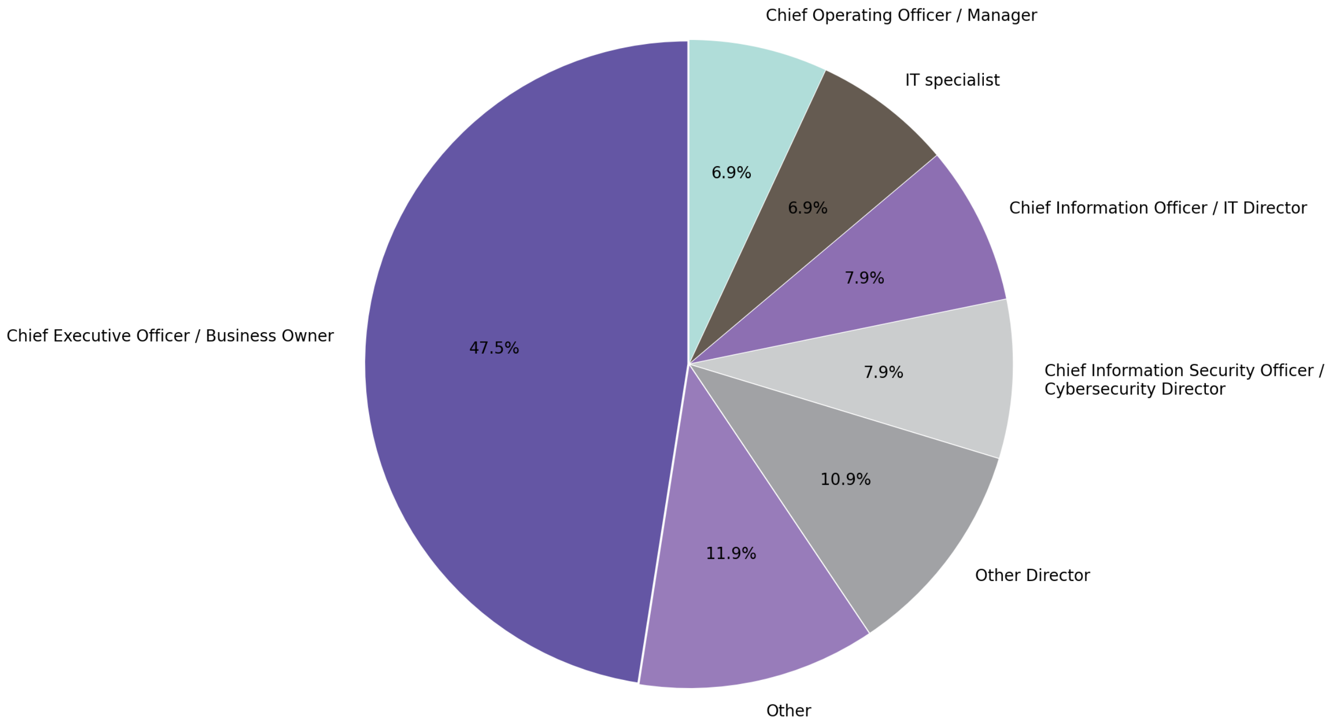


Figure 9: Distribution of answers to the NC3 survey on SMEs' cybersecurity demand by respondents' position within the organization

Q2 – *How many employees does your business have?*

- Fewer than 250 employees: 35 – 34%
- Fewer than 50 employees: 29 – 29%
- Fewer than 10 employees: 30 – 30%
- Only 1 employee: 7 – 7%

Q3 – *In which canton is your head office located?*

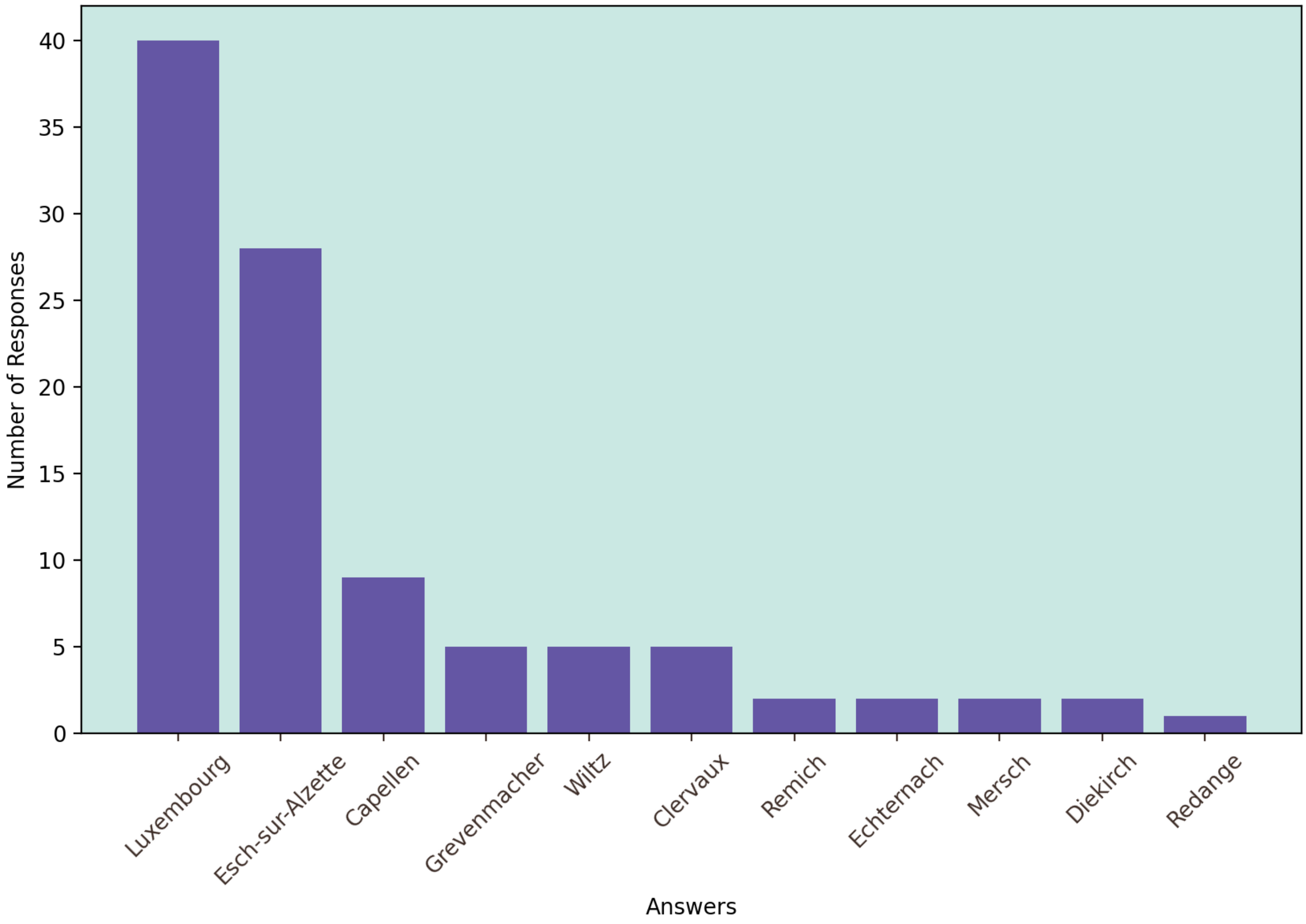


Figure 10: Distribution of answers to the NC3 survey on SMEs' cybersecurity demand by headquarter locations (cantons)

Q4 – *What is your activity sector?*

- NACE Code F – Construction: 28 – 27%
- NACE Code S – Other services activities: 17 – 17%
- NACE Code J – Information and communication: 12 – 12%
- NACE Code C – Manufacturing: 11 – 11%
- NACE Code M – Professional, scientific and technical activities: 8 – 8%
- NACE Code K – Financial and insurance activities: 7 – 7%

- NACE Code K – Wholesale and retail trade; repair of motor vehicles and motorcycles: 5 – 5%
- NACE Code N – Administrative and support service activities: 3 – 3%
- NACE Code H – Transportation and storage: 3 – 3%
- NACE Code L – Real estate activities: 2 – 2%
- NACE Code Q – Human health and social work activities: 2 – 2%
- NACE Code I – Accommodation and food service activities: 1 – 1%
- NACE Code T – Activities of households as employers; undifferentiated goods - and services - producing activities of households for own use: 1 – 1%
- NACE Code R – Arts, entertainment and recreation: 1 – 1%

Enterprise & organization

In examining the cybersecurity practices of SMEs, several key areas have been identified. Most SMEs acknowledge the importance of cybersecurity, yet a significant number lack a dedicated budget for it, highlighting a discrepancy between recognition of its importance and actual financial investment. Decision-making in the event of a cyber incident predominantly falls on the CEO, indicating a centralization of responsibility at the top management level. Regarding work-from-home (WFH) policies, there is a division among respondents on the use of personal devices for remote work, reflecting varying levels of risk acceptance and security measures. Additionally, while the majority of SMEs have not received customer inquiries about their cybersecurity or data protection practices, a noteworthy minority have faced such queries, suggesting varying degrees of external scrutiny and customer expectations in this area.

Q5 – *Is cybersecurity an important topic for your company?*

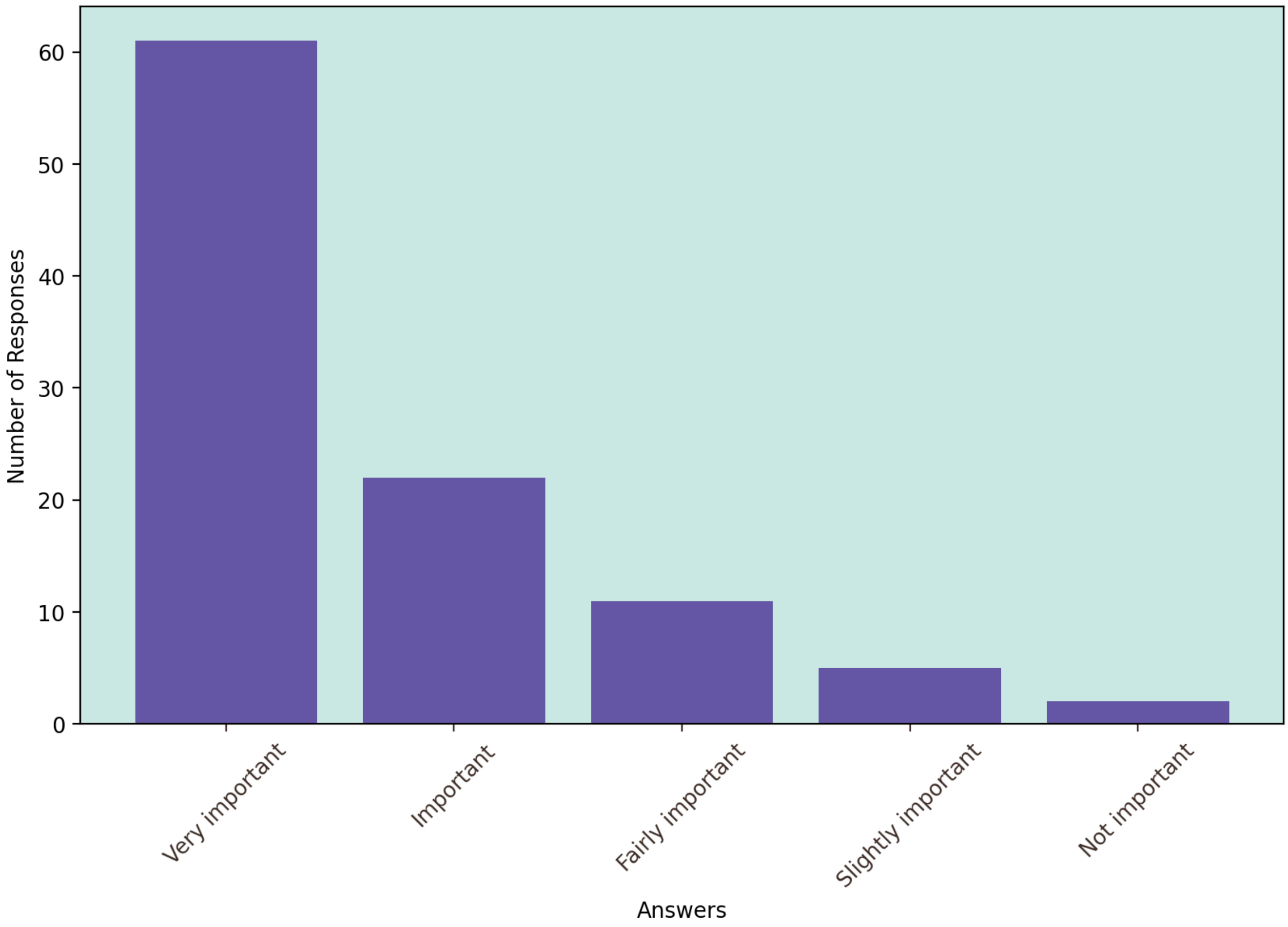


Figure 11: Distribution of answers to the NC3 survey on SMEs' cybersecurity demand by importance of cybersecurity within their organization

Q6 – *Do you have an annual budget dedicated to cybersecurity? If so, how much does that add up to your overall budget?*

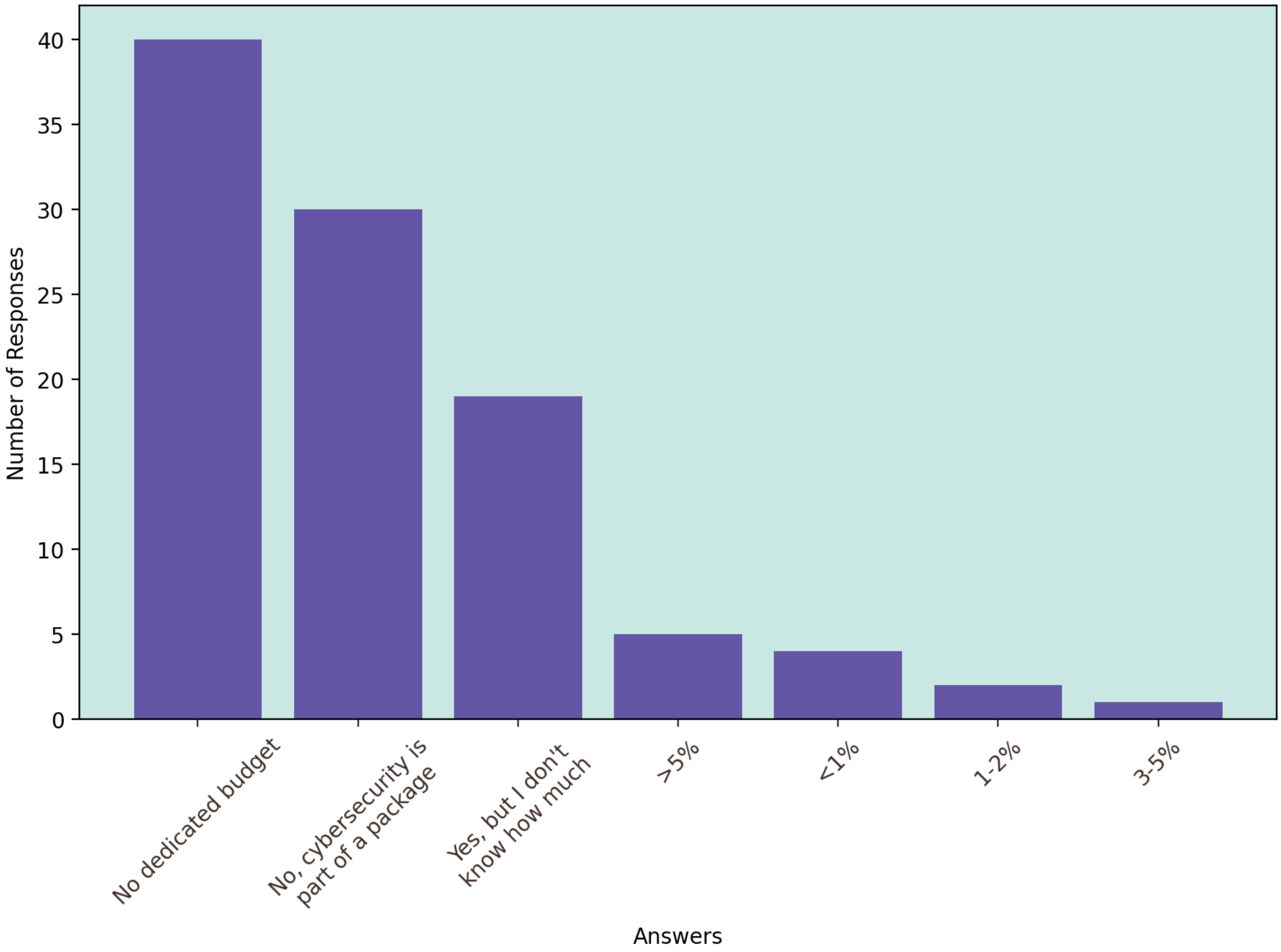


Figure 12: Distribution of answers to the NC3 survey on SMEs' cybersecurity demand by budget

Q7 – *Who is the decision taker regarding cybersecurity in your company?*

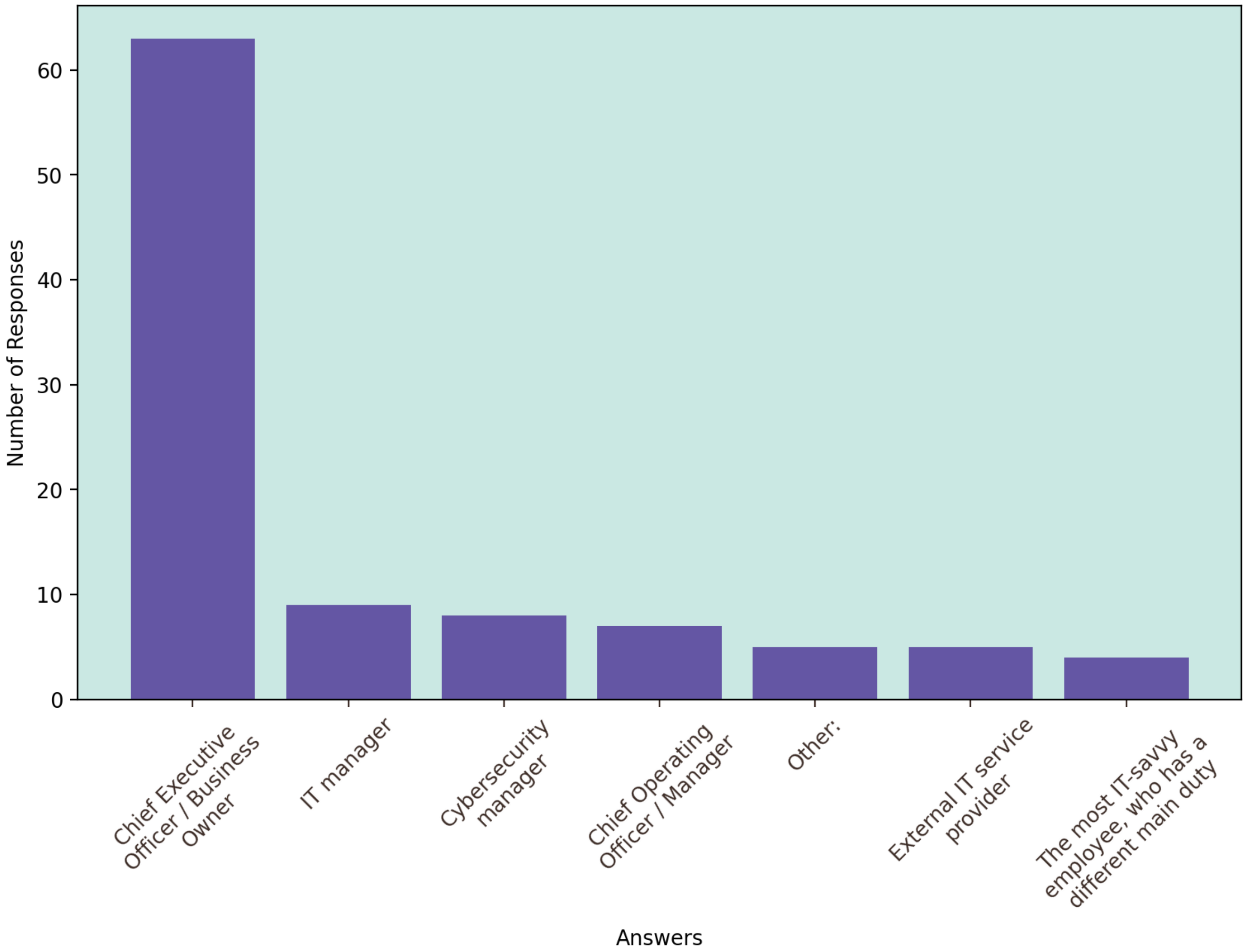


Figure 13: Distribution of answers to the NC3 survey on SMEs' cybersecurity demand by decision taker

Q8 – *Your employees are allowed to work…*

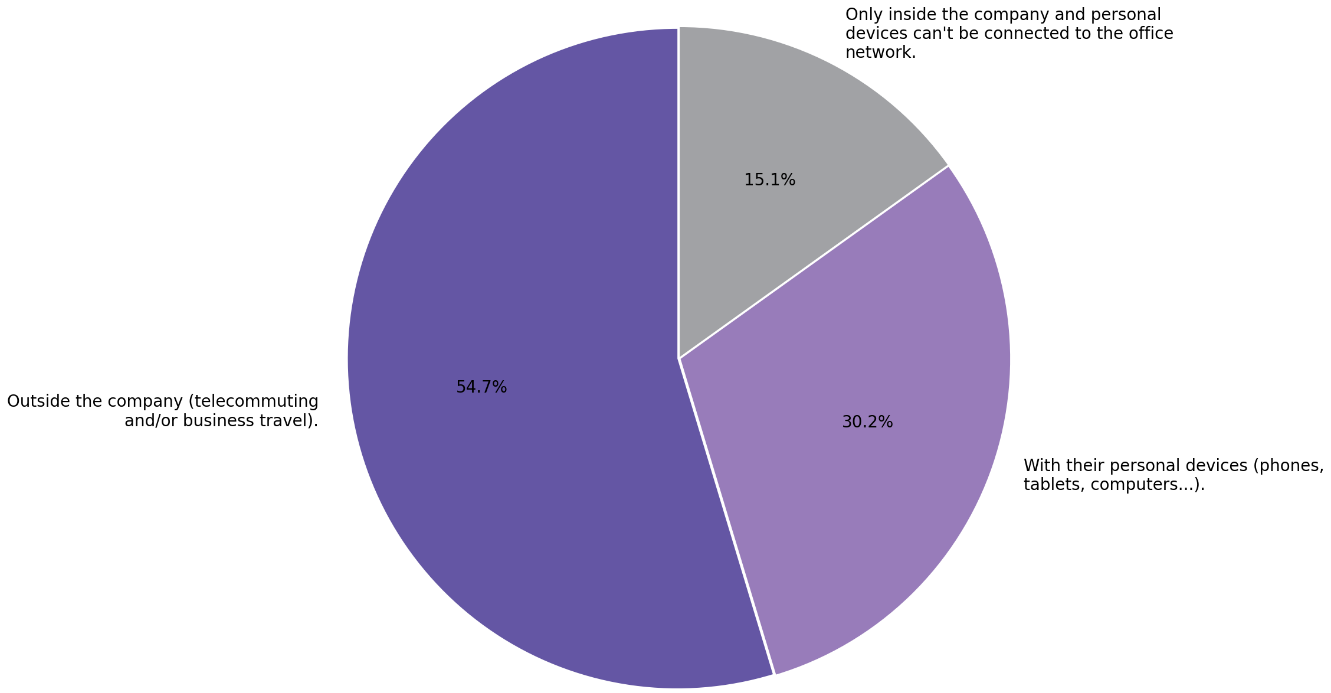


Figure 14: Distribution of answers to the NC3 survey on SMEs’ cybersecurity demand by employees digital practices

Q9 – *Are your employees allowed to use their personal devices (phones, tablets, computers) for work?*

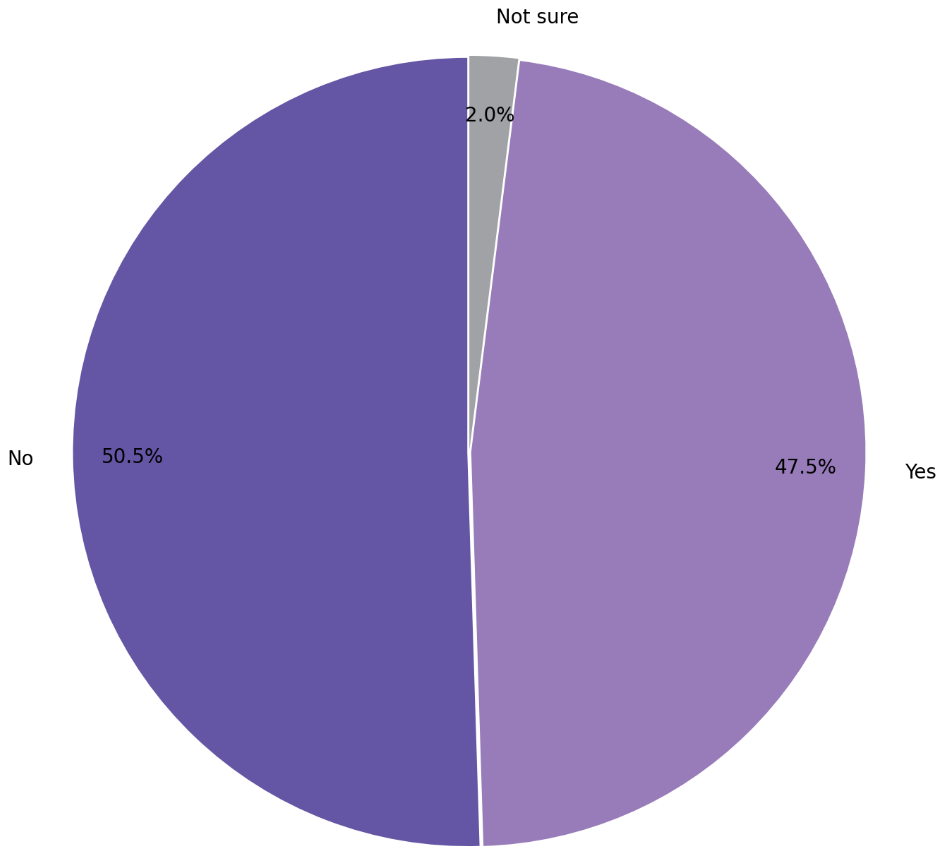


Figure 15: Distribution of answers to the NC3 survey on SMEs' cybersecurity demand by employee authorization to use personal devices for work

Q10 – *Did you ever get questions from your customers about...*

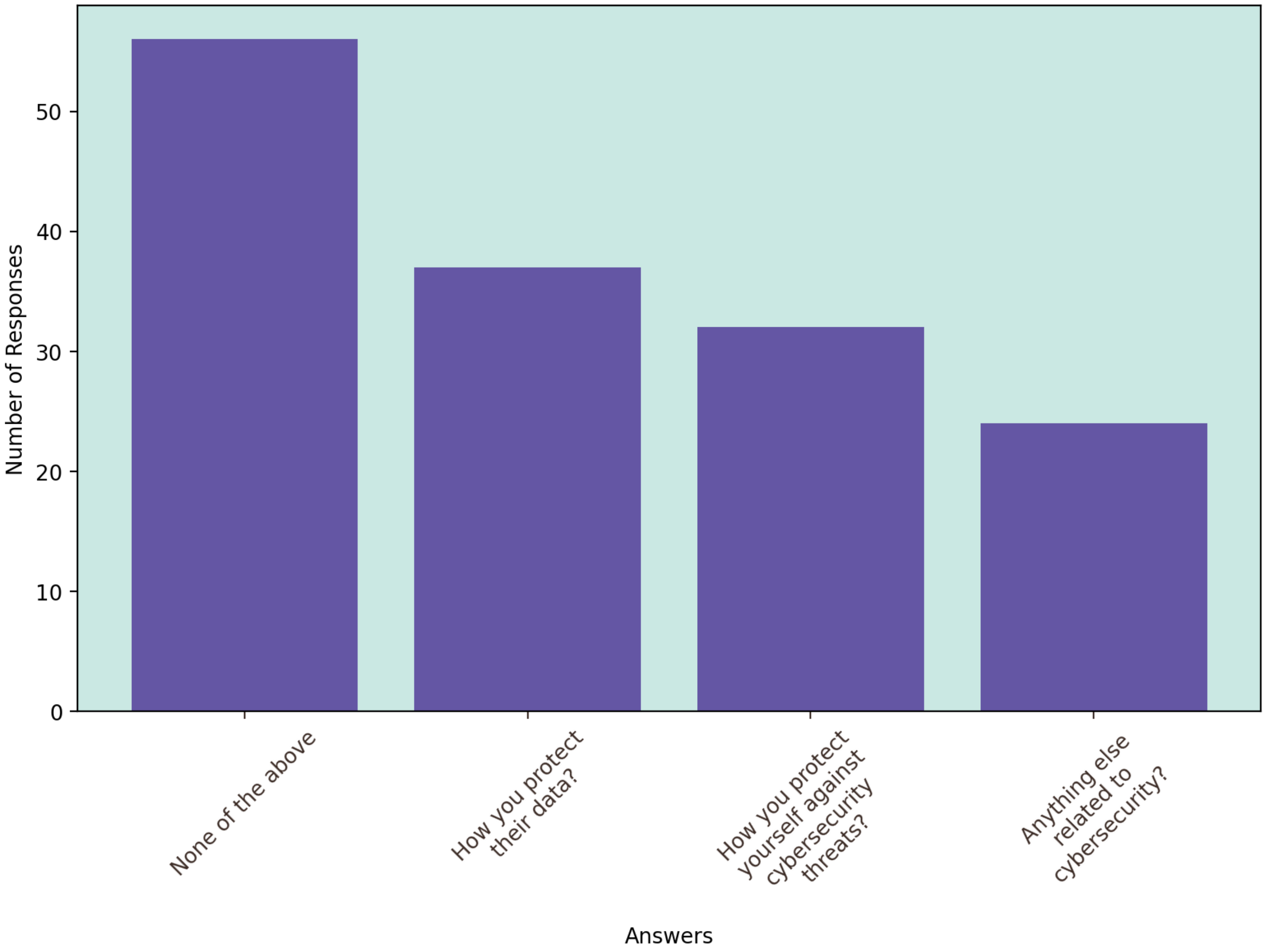


Figure 16: Distribution of answers to the NC3 survey on SMEs' cybersecurity demand by customer questions on cybersecurity or data protection

Skills & awareness

This section explores the relationship between digital skills, training, and the confidence level of respondents in handling cybersecurity challenges. It reveals that while a significant portion of respondents indicated their employees have not undergone any cybersecurity awareness training to identify and respond to potential risks, many had received such training a year ago, with others only partially trained. In terms of confidence in managing cyber incidents, most respondents expressed moderate confidence (38.6%), followed closely by those who reported high confidence (35.6%). A notable 32.4% of respondents have pursued self-study in cybersecurity, while 26.8% have participated in training or awareness events organized by professional chambers. However, 25.4% reported having no training in this area. Additionally, the majority of SMEs participating in the survey indicated that they have at least one employee with computer skills, underscoring the prevalence of basic digital competence in the workforce.

Q11 – *Have your employees undergone any cybersecurity awareness training to help them identify and respond to potential risks?*

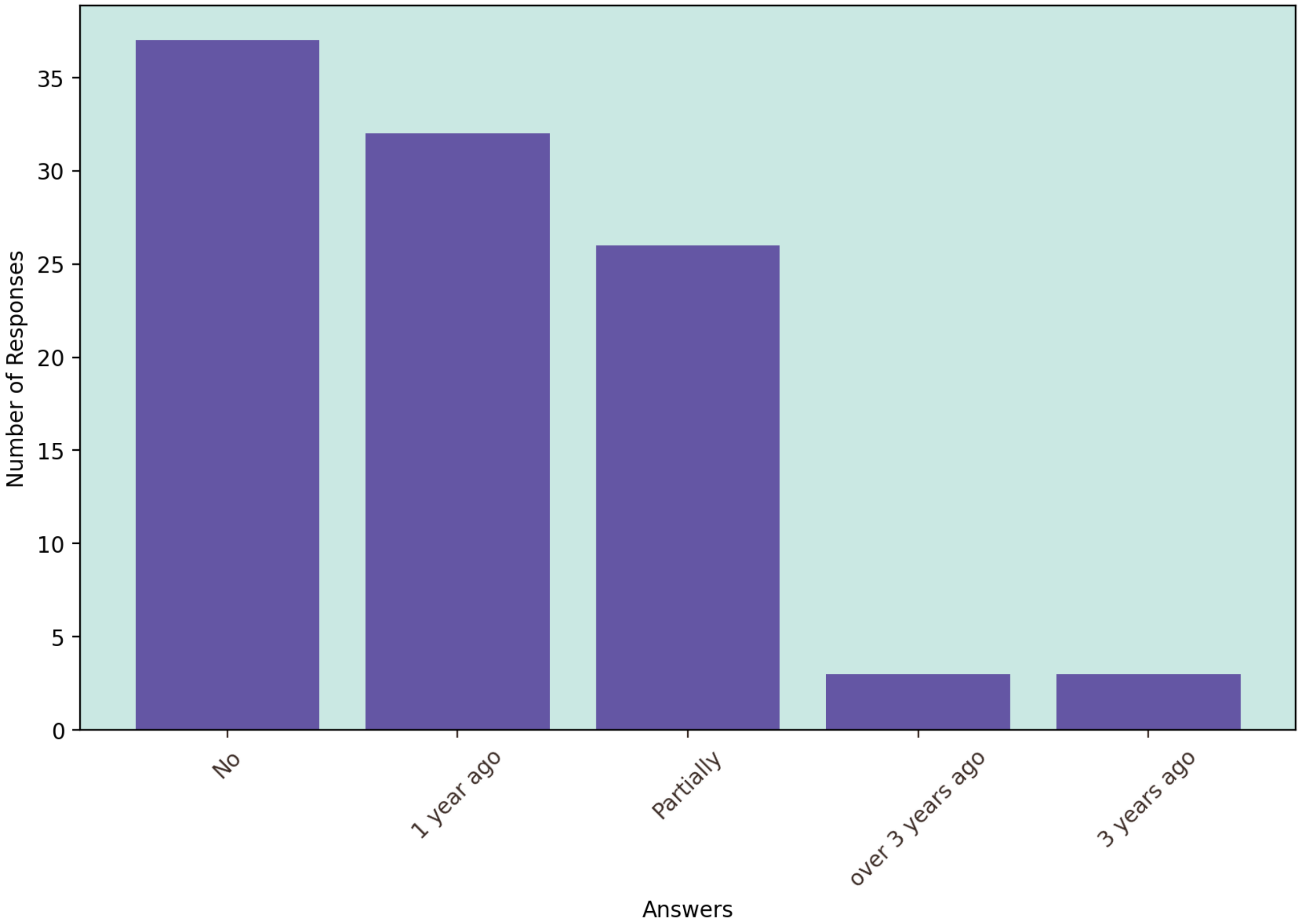


Figure 17: Distribution of answers to the NC3 survey on SMEs' cybersecurity demand by employee training

Q12 – *What's your confidence level in dealing with cybersecurity?*

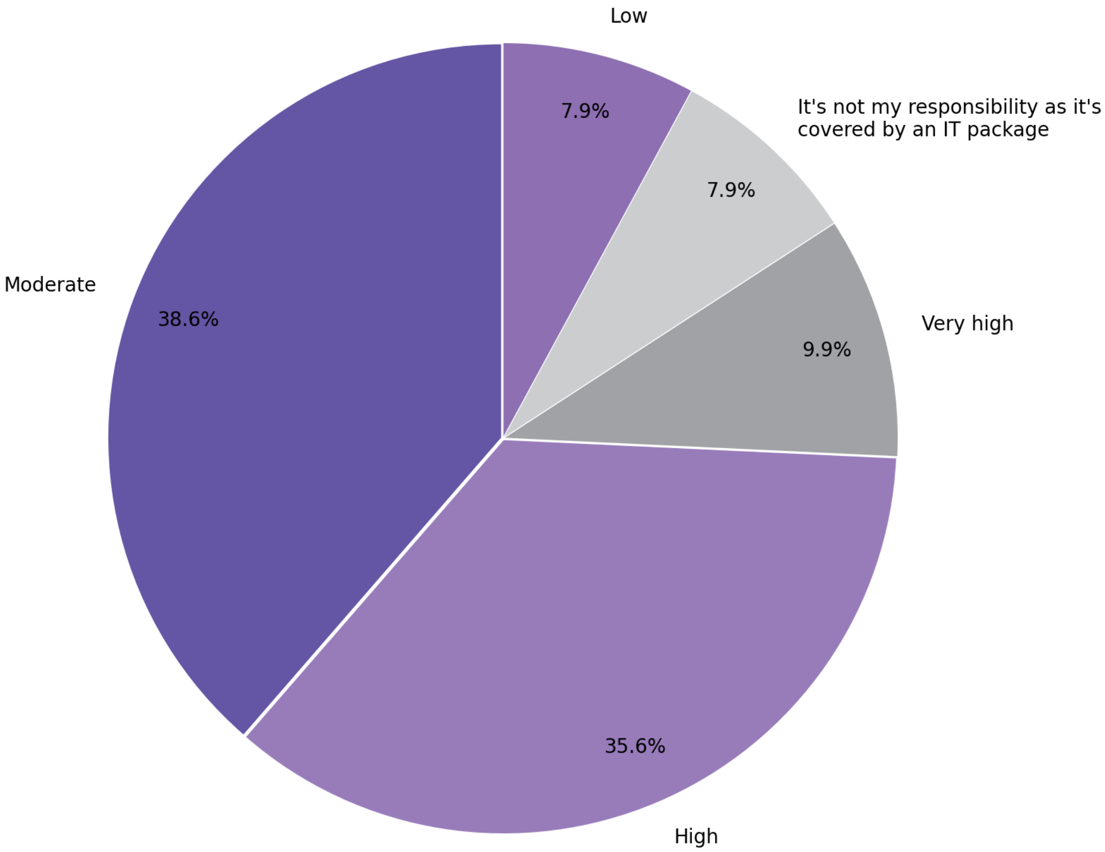


Figure 18: Distribution of answers to the NC3 survey on SMEs' cybersecurity demand by confidence level of respondent

Q13 – *Have you personally received cybersecurity training?*

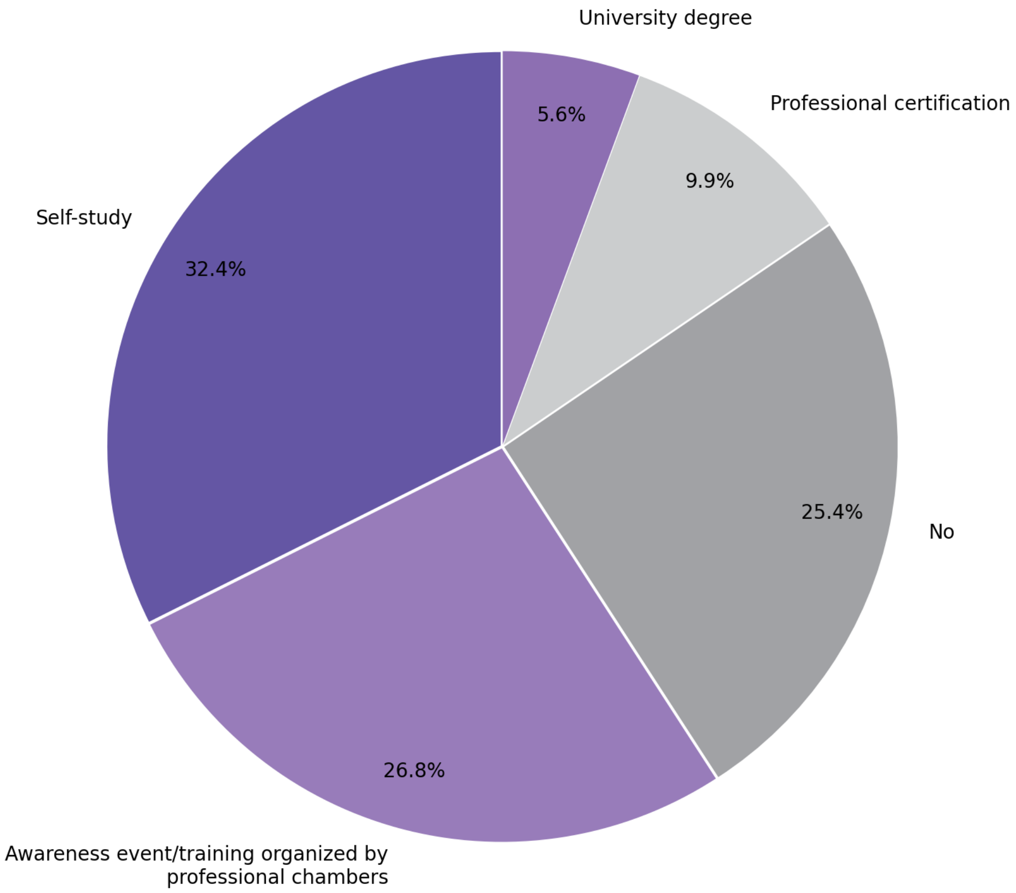


Figure 19: Distribution of answers to the NC3 survey on SMEs' cybersecurity demand by respondent training

Q14 – *Do you have one or more employees with computer skills?*

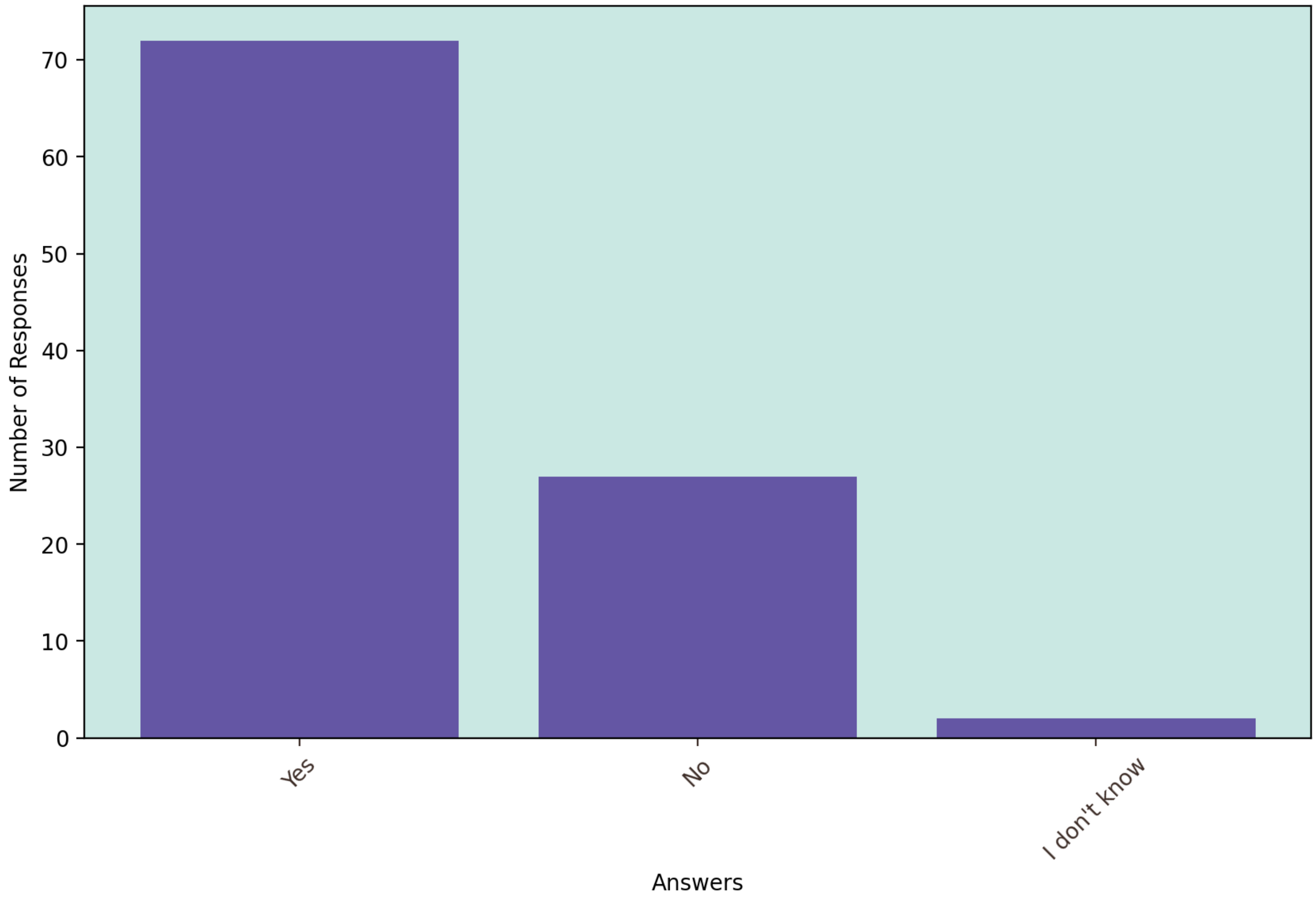


Figure 20: Distribution of answers to the NC3 survey on SMEs' cybersecurity demand by employee with computer skills

Digital services and products

The focus of this section is on the various digital tools and platforms that SMEs employ, along with the cybersecurity solutions they implement. Communication tools are the most commonly used among these companies, followed by accounting and management tools. Key tools in this category include mailboxes, websites, videoconferencing, and social networks, which are essential for SME operations. Accounting software and electronic invoicing also see significant usage. Furthermore, a considerable number of SMEs utilize CRM (Customer Relationship Management), order management, and appointment scheduling software, highlighting their commitment to customer service and organizational efficiency. The adoption of cloud solutions indicates a trend towards more digitally oriented data storage and management. In specific sectors, tools like ICAD/CAD software, IIOT (Industrial Internet of Things), and advanced robotics are frequently used, particularly in manufacturing. As for cybersecurity, antivirus software is the most prevalent solution, complemented by unique passwords for each device and service, data backup solutions, VPNs (Virtual Private Networks), and access management systems, indicating a fairly high level of integration of basic digital asset security solutions in SMEs.

Q15 – *In which areas are you using digital tools/platforms in your company?*

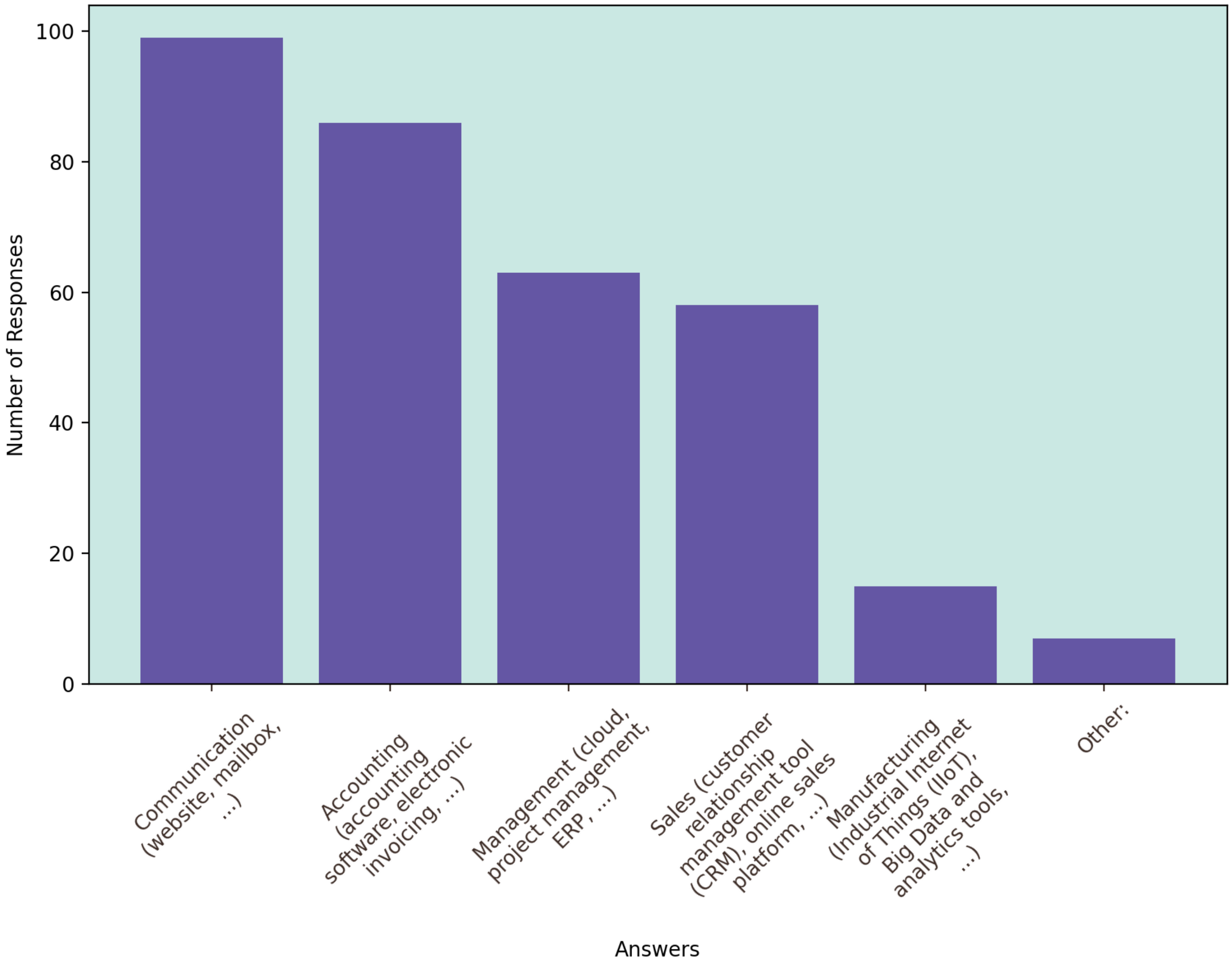


Figure 21: Distribution of answers to the NC3 survey on SMEs' cybersecurity demand by digital tools

Q16 – *As you use digital tools for communication, could you specify which kind?*

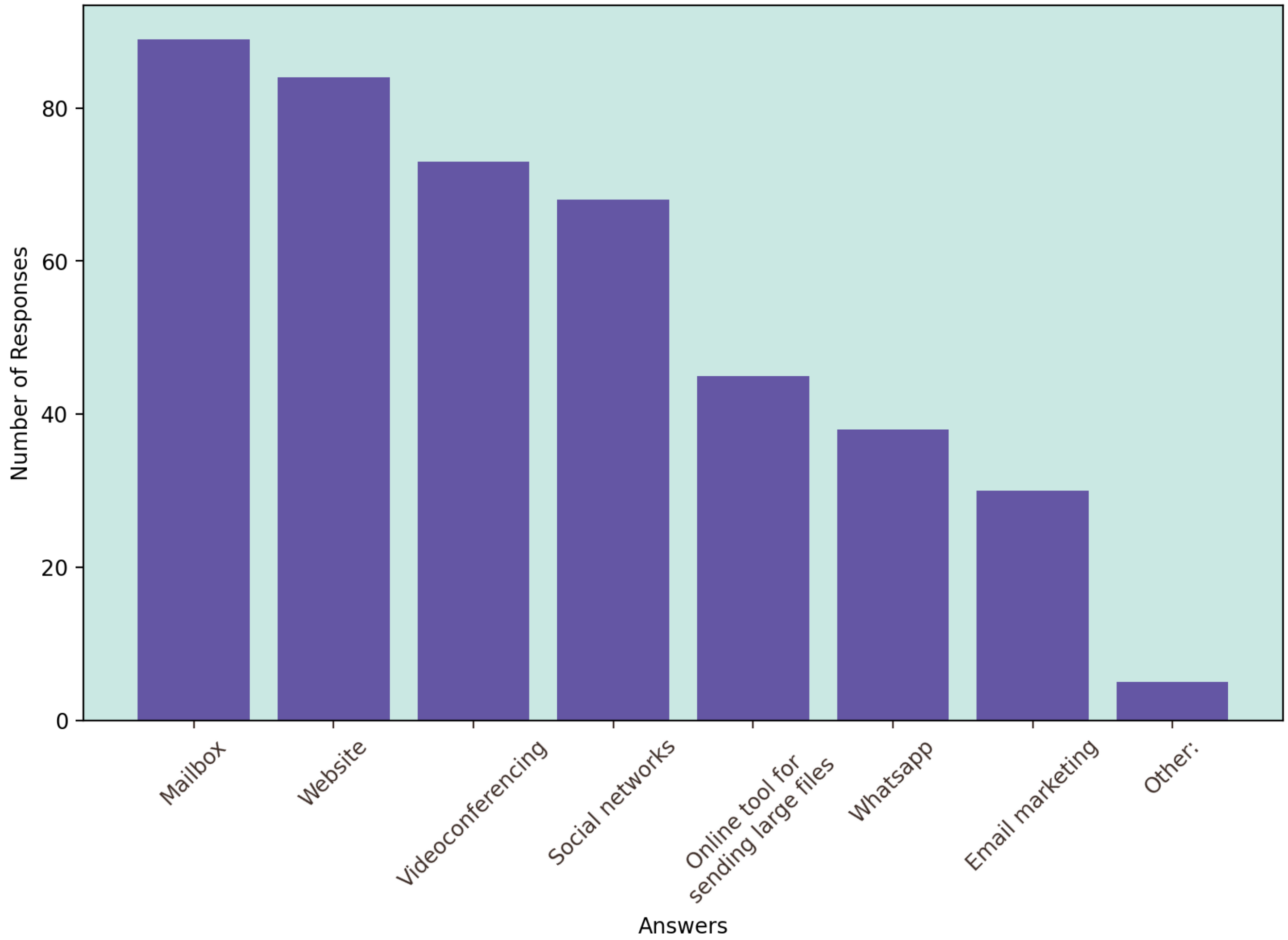


Figure 22: Distribution of answers to the NC3 survey on SMEs' cybersecurity demand by digital tools for communication

Q17 – *As you use digital tools for accounting, could you specify which kind?*

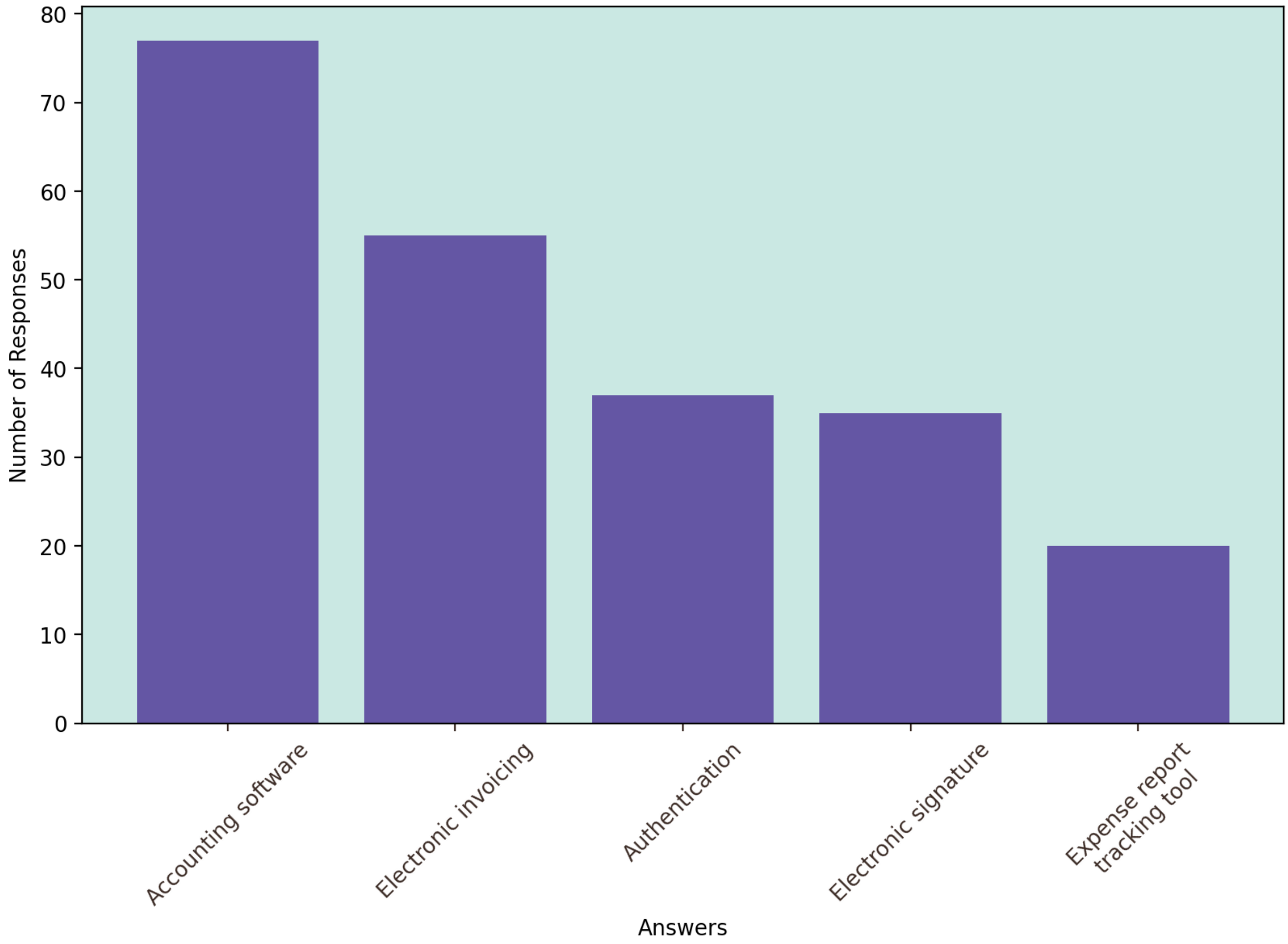


Figure 23: Distribution of answers to the NC3 survey on SMEs' cybersecurity demand by digital tools for accounting

Q18 – *As you use digital tools for sales, could you specify which kind?*

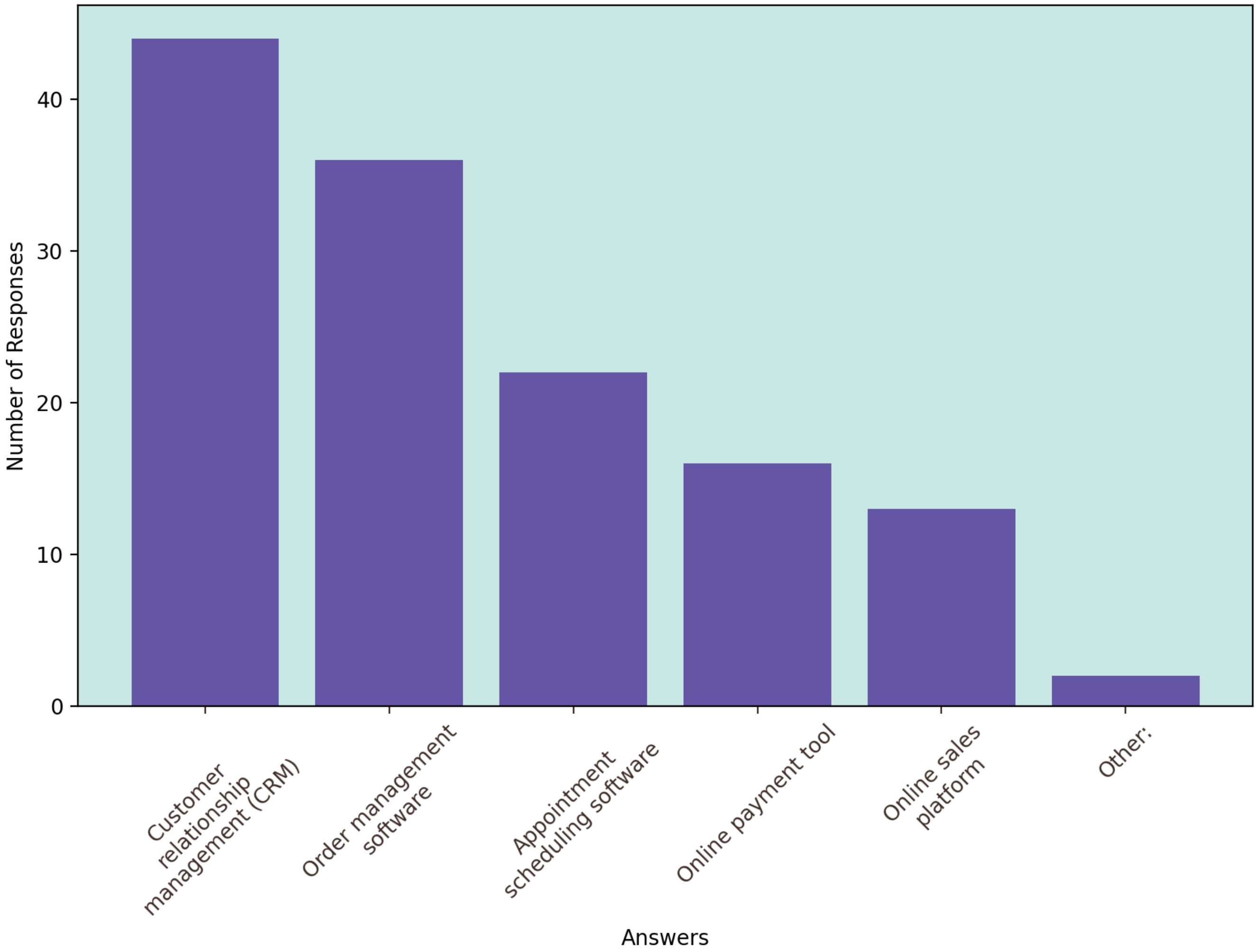


Figure 24: Distribution of answers to the NC3 survey on SMEs' cybersecurity demand by digital tools for sales

Q19 – *As you use digital tools for management, could you specify which kind?*

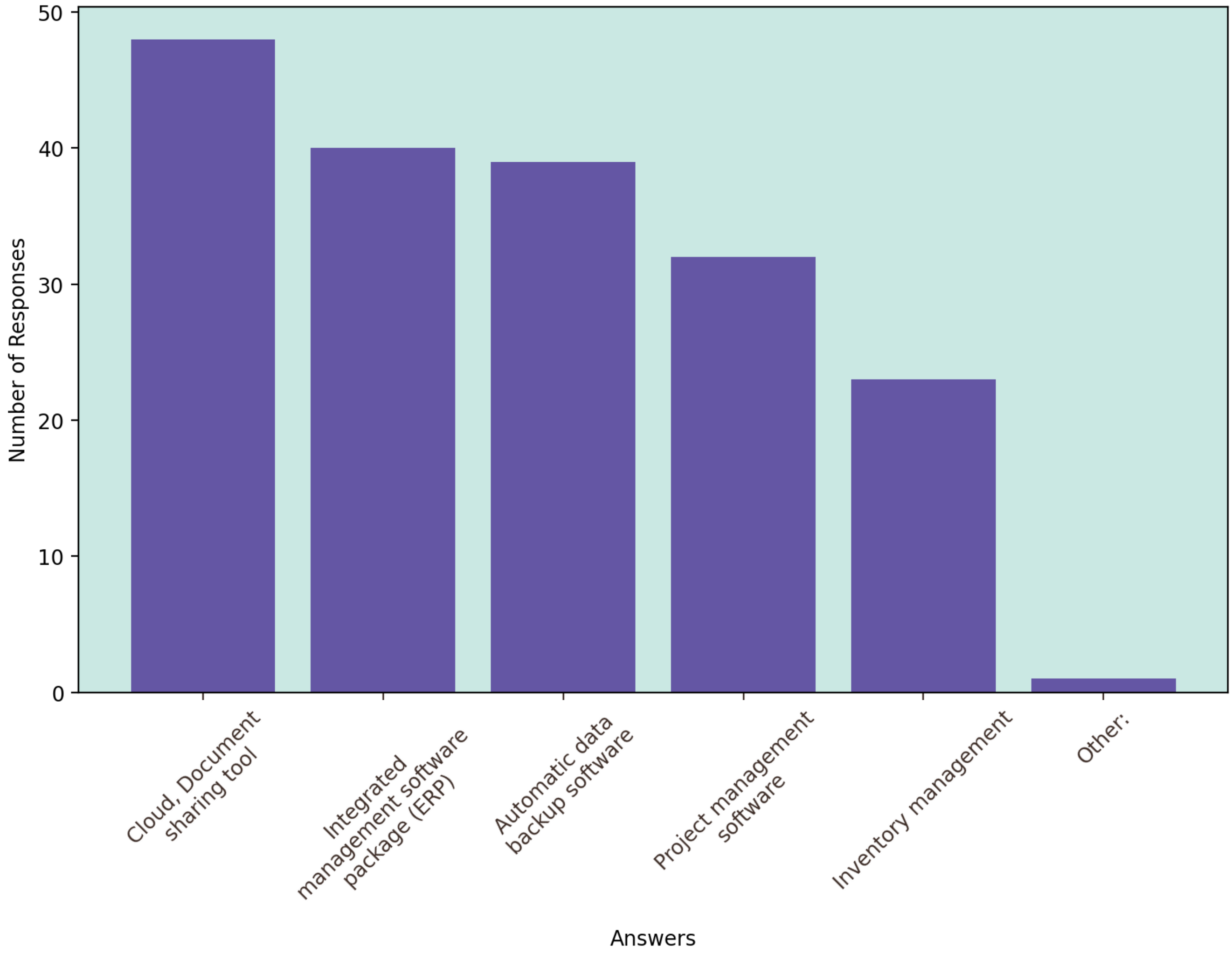


Figure 25: Distribution of answers to the NC3 survey on SMEs' cybersecurity demand by digital tools for management

Q20 – *As you use digital tools for manufacturing, could you specify which kind?*

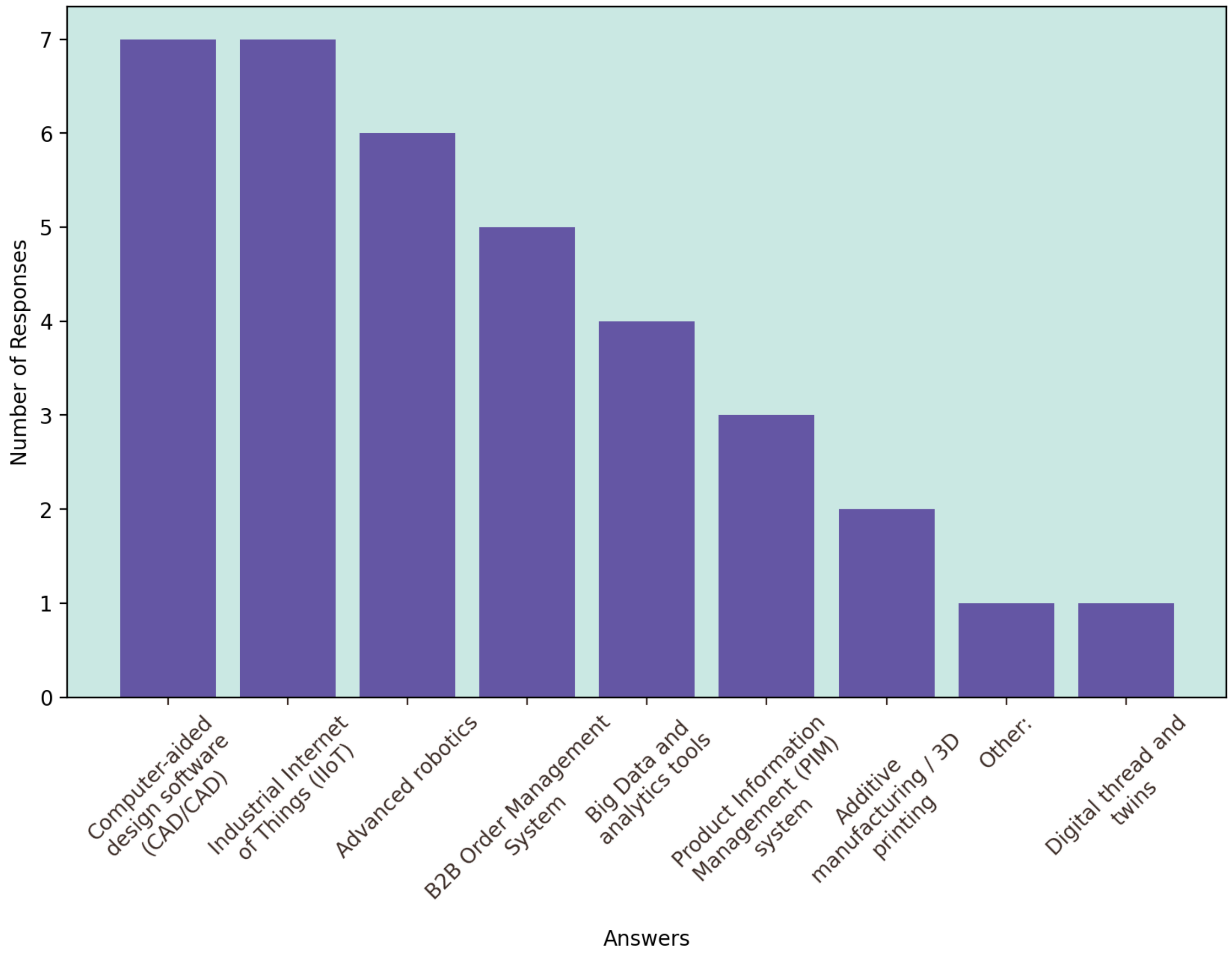


Figure 26: Distribution of answers to the NC3 survey on SMEs' cybersecurity demand by digital tools for manufacturing

Q21 – *Does your company use any of the following cybersecurity solutions?*

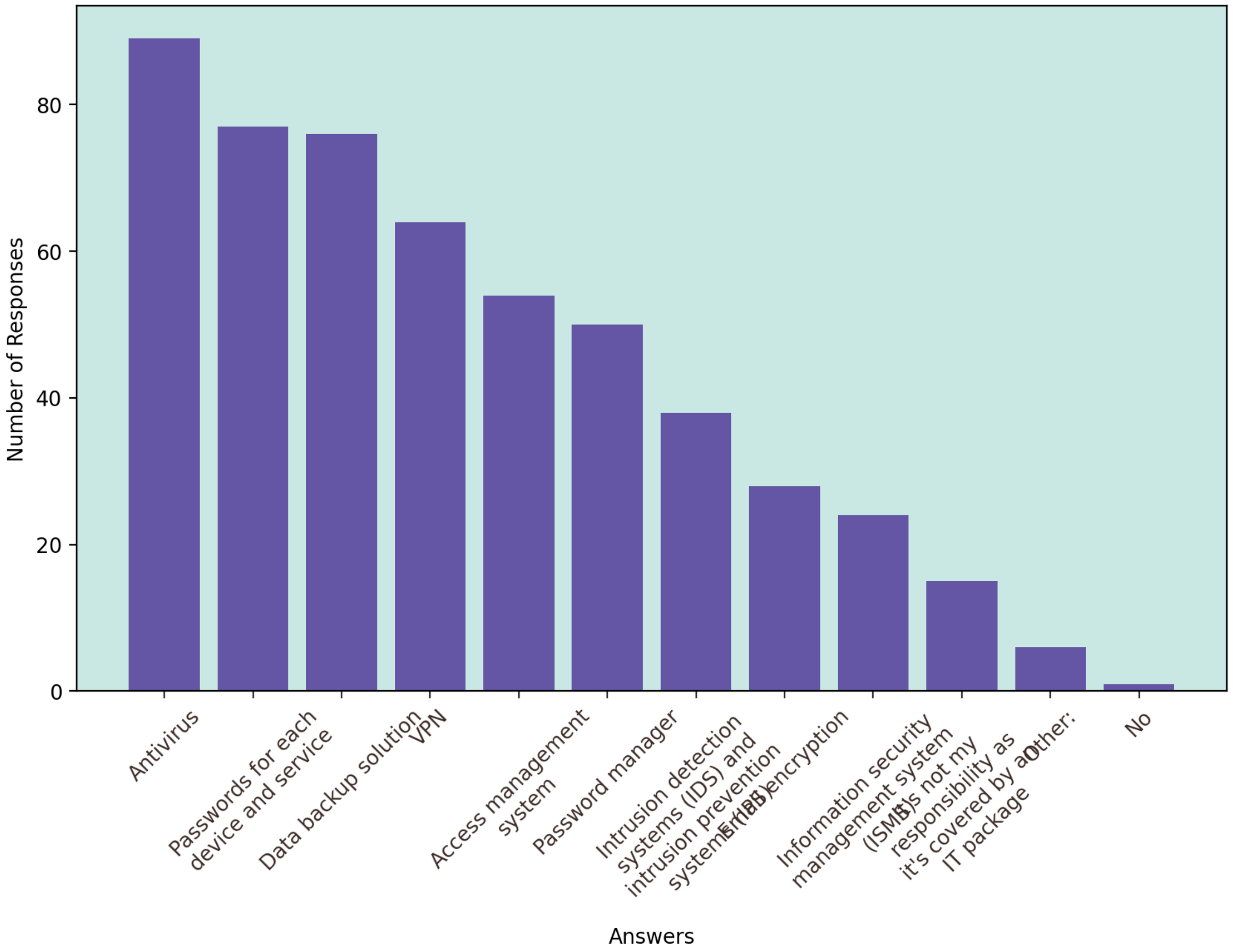


Figure 27: Distribution of answers to the NC3 survey on SMEs' cybersecurity demand by cybersecurity solutions

Market & solutions

Exploring the practices of SMEs in their interactions with market players and their approaches to evaluating and acquiring products reveals insightful trends. A significant number of respondents depend on IT consultants who are not affiliated with their internet service providers, while in-house IT and cybersecurity experts, along with internet cybersecurity providers, also play crucial roles. In seeking support for cybersecurity, most SMEs prefer professional organizations, followed closely by public sector organizations and independent cybersecurity consultants. Factors influencing the adoption of cybersecurity services or solutions predominantly include news, peer information sharing, and advice from IT service providers, with legal constraints being another key factor. For SMEs that have faced cyber incidents, legal constraints emerge as the foremost driver of adoption, succeeded by advice from IT service providers and the experience of the incident itself. Evaluation criteria for cybersecurity services are centered around the seller's trustworthiness, cost, ease of use, technical specifications, and the comprehensiveness of the solution. As for satisfaction levels with available cybersecurity services, 44.6% of respondents express satisfaction, but a notable 36.6% remain uncertain. Confidence levels in their digital service providers vary, with half of the SMEs reporting high confidence (48.5%), and others displaying moderate (16.8%) or very high (15.8%) confidence.

Q22 – *Who supports you to manage your cybersecurity?*

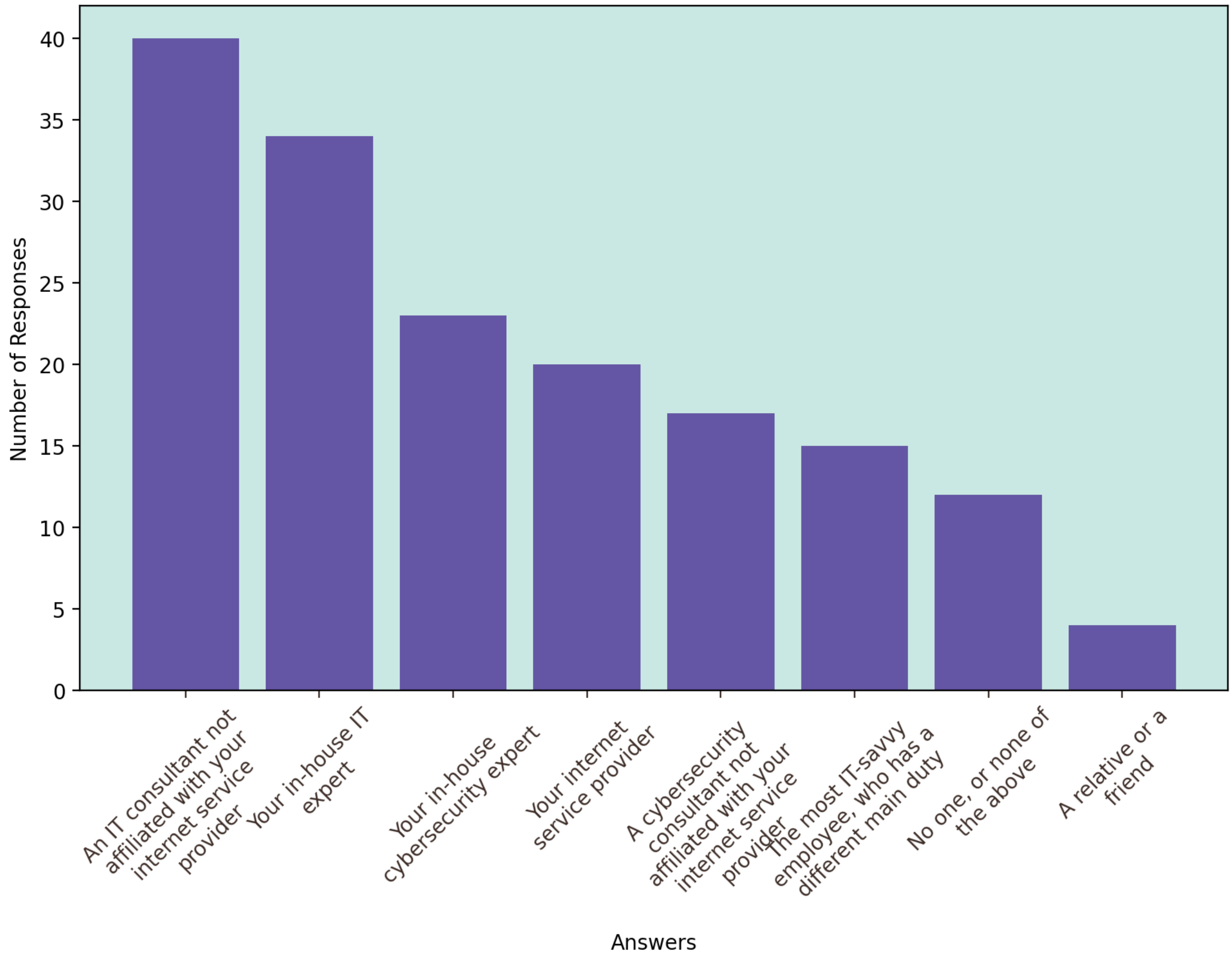


Figure 28: Distribution of answers to the NC3 survey on SMEs' cybersecurity demand by responsible party

Q23 – *Are there any specific organizations or partners that you would like to collaborate with for cybersecurity support?*

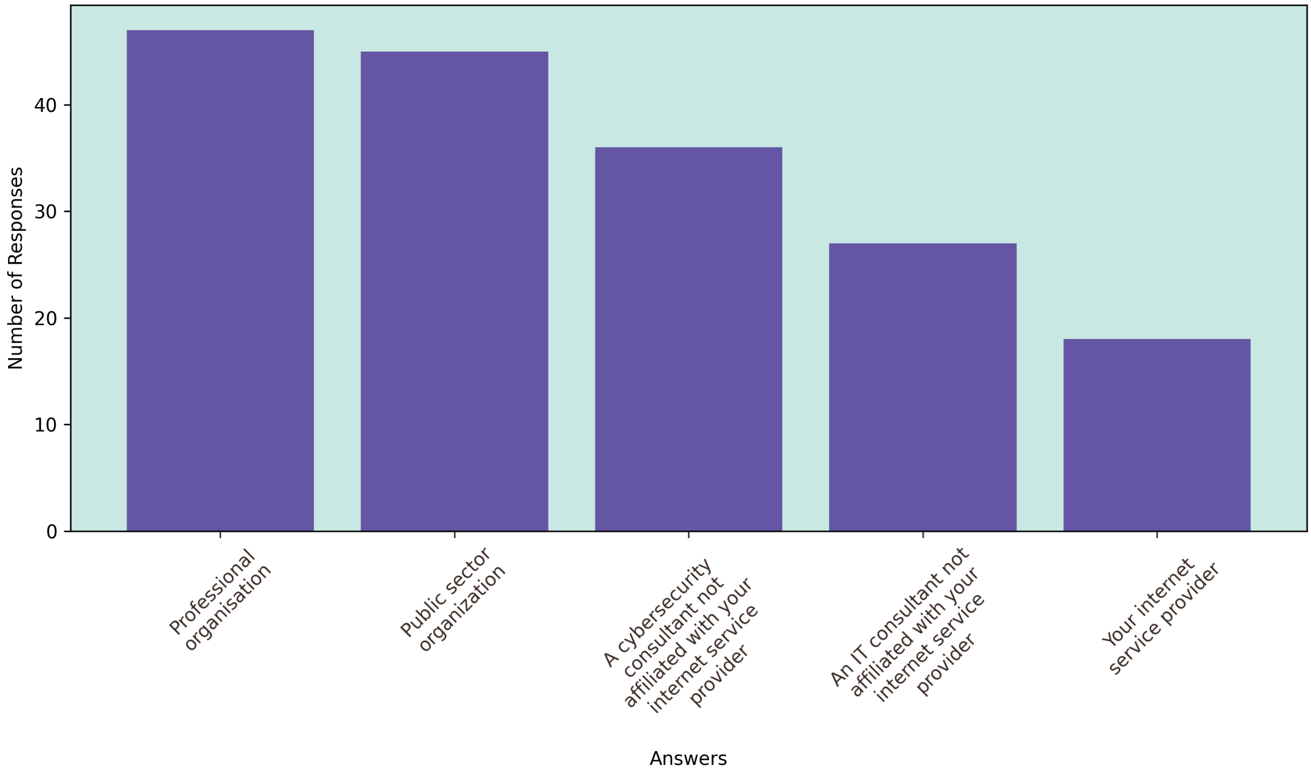


Figure 29: Distribution of answers to the NC3 survey on SMEs' cybersecurity demand by expectations in terms of cybersecurity support

Q24 – *What are your key drivers in the adoption of cybersecurity services or solutions?*

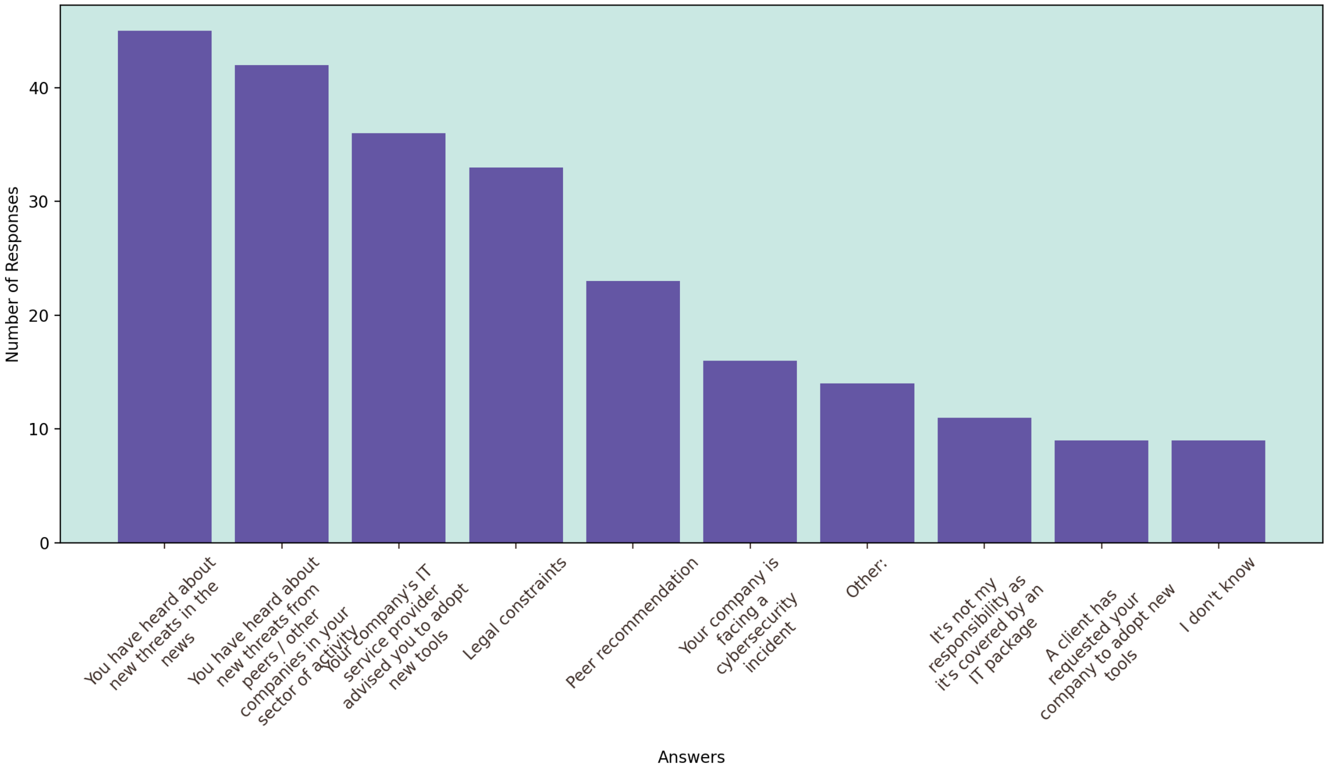


Figure 30: Distribution of answers to the NC3 survey by key drivers in the adoption of cybersecurity services or solutions

Impact of a cyber incident on the key drivers in the adoption of cybersecurity services or solutions.

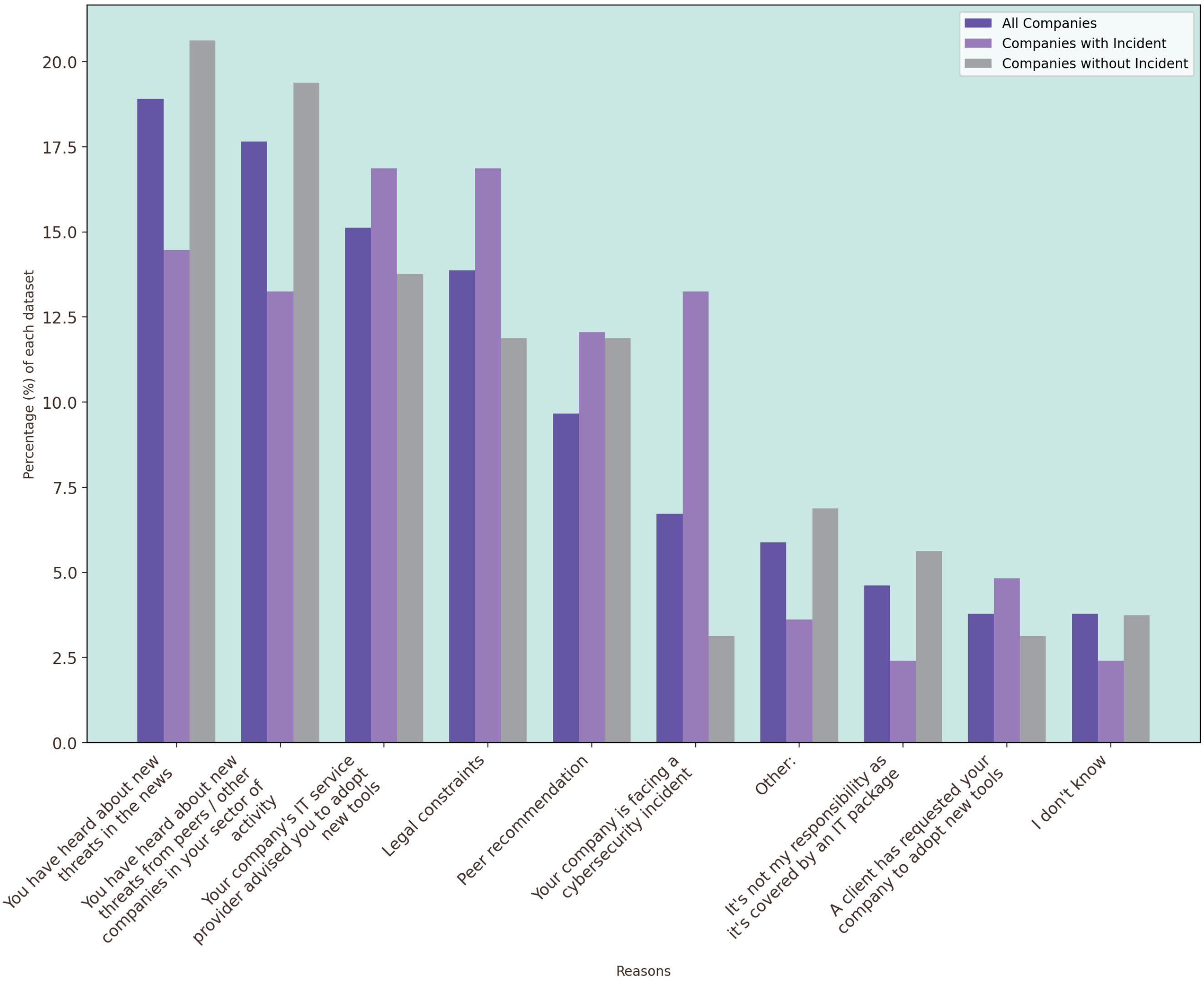


Figure 31: Figure Distribution of answers in the survey comparing key drivers of adoption of cybersecurity services or solutions between companies that had an incident, companies without incident, and the total number of respondents

Q25 – *What are your criteria for evaluating cybersecurity services or solutions?*

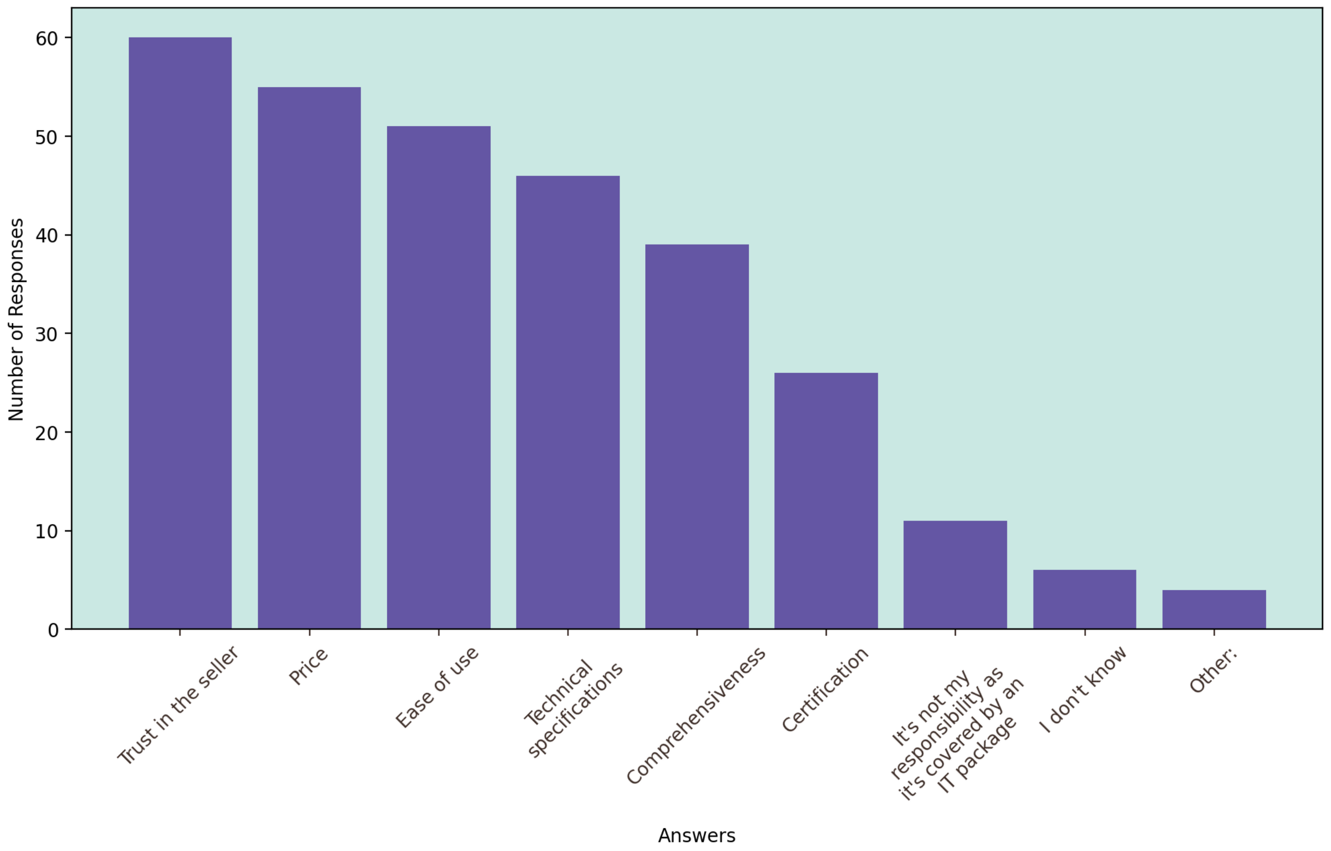


Figure 32: Distribution of answers to the NC3 survey by criteria for evaluating cybersecurity services or solutions

Q26 – *Do the cybersecurity services available on the market suit your needs?*

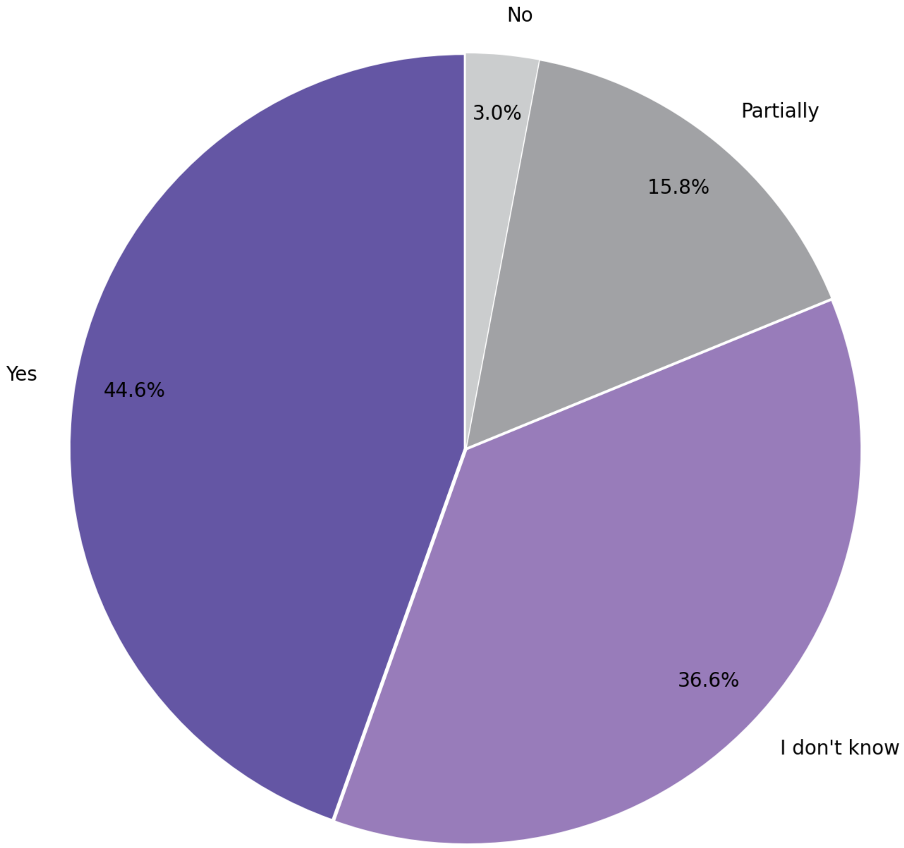


Figure 33: Distribution of answers to the survey by satisfaction with cybersecurity services available on the market

Q27 – *How trustworthy would you evaluate your digital service provider(s)?*

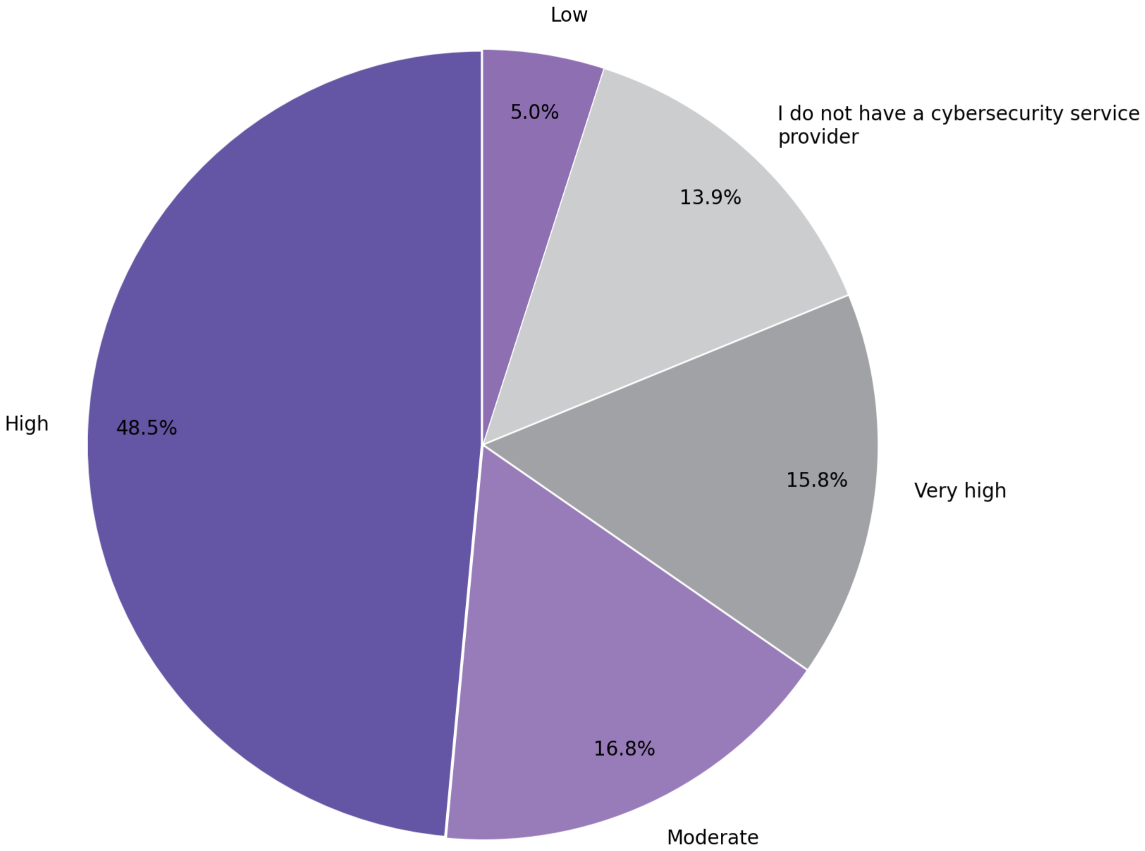


Figure 34: Distribution of answers to the survey by level of trust in respondent digital service provider(s)

Incident

In studying the incidence and nature of cyber attacks against businesses, our research focuses on the number of companies that have suffered such attacks, the methods employed, and their impact. A notable 58.7% of respondents indicated that they had not encountered any cyberattacks. However, among those that did, phishing emails emerged as the most common attack vector (15.6%), followed by incidents of unknown origin, data breaches, and attacks initiated through company devices, each accounting for 5.5%. The majority of affected companies cited employee time loss as the primary consequence, along with direct financial losses, asset/material loss, and personal data breaches.

Q28 – *Has your company, to your knowledge, been the victim of a cyberattack?*

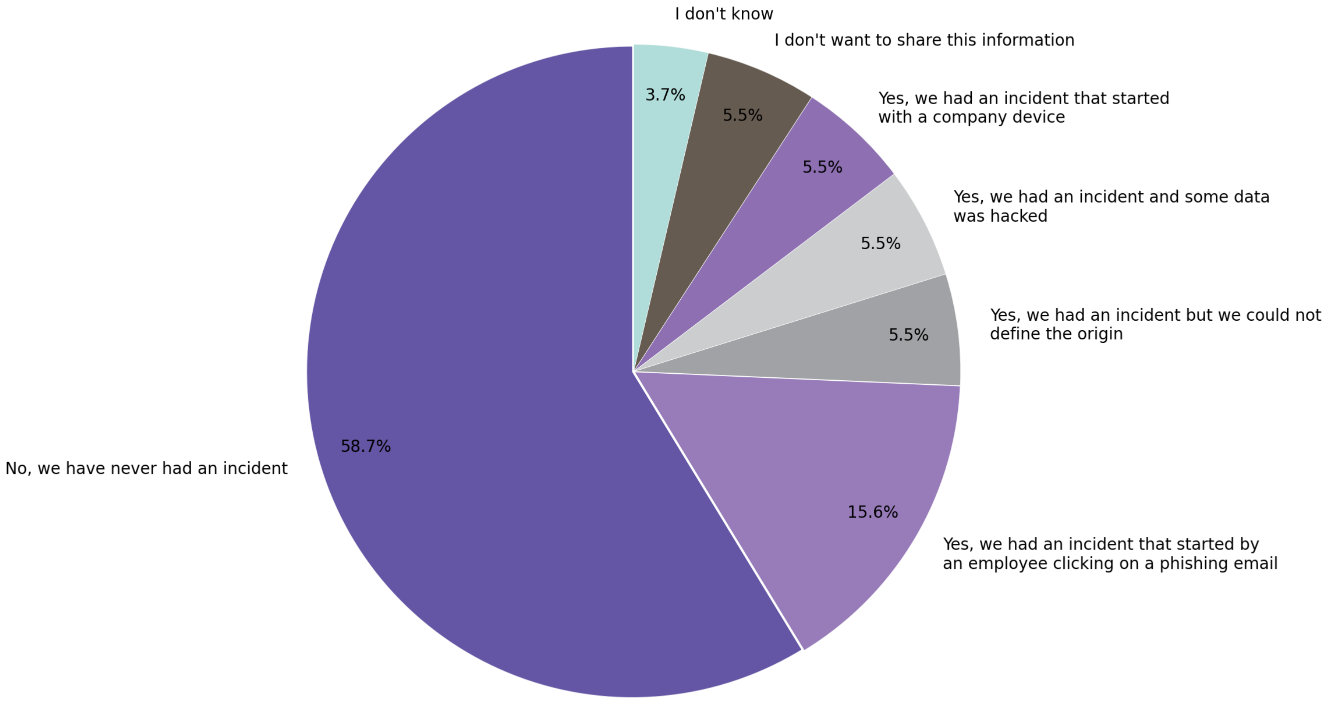


Figure 35: Distribution of answers to the survey by incident

Q29 – *What impact did the cyberattack have on your company?*

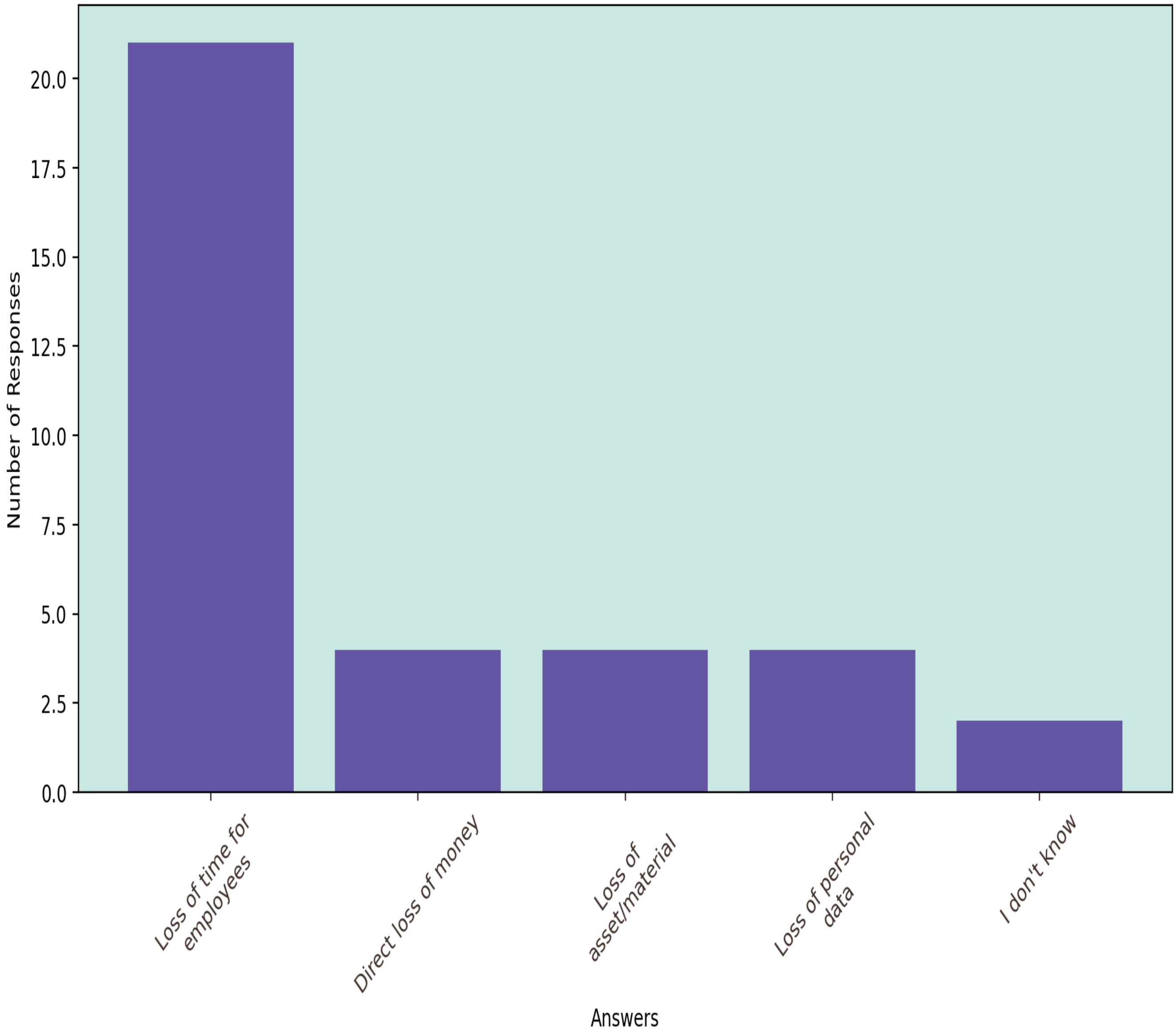


Figure 36: Distribution of answers to the survey by incident

Regulations

In examining the awareness of the legal framework within which SMEs operate, particularly in terms of cybersecurity, our survey reveals that most companies expressed confidence in their understanding of the regulations pertaining to cybersecurity competencies, situations, and services. However, this confidence is closely matched by a significant number of respondents acknowledging a deficiency in their understanding of cybersecurity obligations. Additionally, there is a smaller yet noteworthy proportion of respondents who indicated a lack of information regarding their data protection obligations.

Q30 – *From a regulatory point of view, do you think you lack information regarding...*

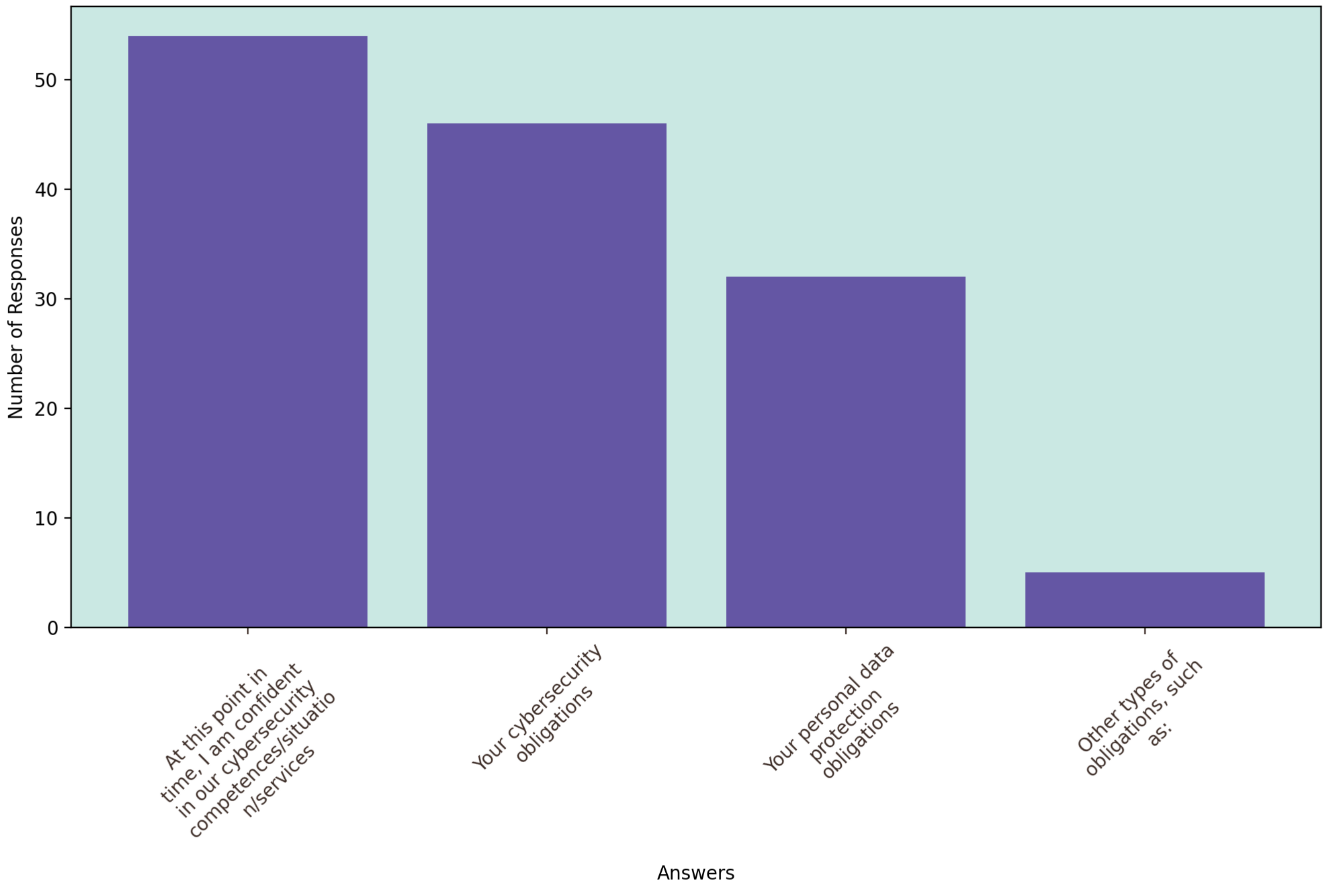


Figure 37: Distribution of answers to the survey by need of information about regulations

Certification

The final part of our analysis delves into SMEs' interest in obtaining cybersecurity certification as a means to structure their cybersecurity approach. It reveals that a substantial majority (80.2%) of the respondents do not currently pursue such certification. Additionally, a smaller segment of respondents is unsure about whether their company holds a cybersecurity certification. Only a minor fraction (6.9%) of the surveyed SMEs actually have such a certification in place.

Q31 – *Does your company have a cybersecurity certification?*

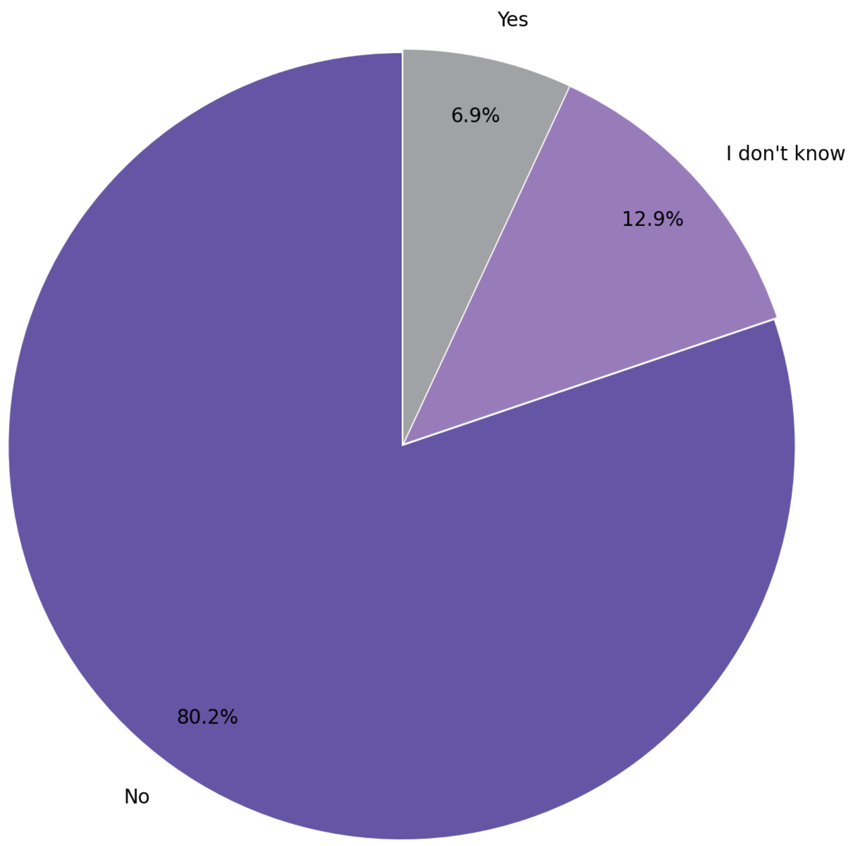


Figure 38: Distribution of answers to the survey according to whether the company has cybersecurity certification

4 – Insights from focus group discussion with SME representatives

For a more comprehensive view of the market, alongside distributing the survey through professional organizations and chambers, a focus group was convened with SME representatives on June 20, 2023. This offered a qualitative dimension to the research, facilitating an open exchange of experiences beyond the survey's scope. The focus group discussions were structured around the survey questions to maintain consistency. Participants, recruited through the project's institutional partners, contributed insights under the assurance of confidentiality. Only minimal, non-identifiable information about the participants is disclosed in this report.

Participants:

- 2 Construction companies (each with between 200 and 250 employees)
- 1 Engineering company (around 150 employees)

- 1 Automotive Garage (around 50 employees)

Below is a summary of the discussions, including the key findings, organized by the same categories listed in the survey:

Enterprise & organization

- Allocating funds for cybersecurity tools is relatively straightforward due to increasing threat awareness, although these budgets often fold into the broader IT budget.
- Heightened awareness among business leaders has led to significant budget increments for cybersecurity.
- No customers explicitly asked participants about their practices in terms of cybersecurity or data protection.

Skills and awareness

- Cybersecurity awareness has grown significantly over the past five years, fueled by news and incidents of cyberattacks in Luxembourg or affecting companies close to the participants. However, awareness levels vary according to the degree of digitization of their respective sectors.
- Training is rare, particularly in the absence of dedicated internal security resources and a dedicated IT function. However, informal practices of sharing information on potential risks such as phishing attempts have been adopted.
- Training and awareness programs are most effective when grounded in real-life scenarios and direct personal or professional impact.
- Executives lack confidence in managing a cyberattack unless they have in-house IT and cybersecurity expertise or past successful response experience.
- Participants demonstrate a significant divergence in their approach to internal and external security. While external security measures seem well-understood and managed, internal security remains vulnerably addressed.

Digital services and products

- The rise of digitization in various sectors is directly linked to a growing awareness of security risks, particularly in terms of business interruptions and data loss.
- All participating companies had a minimal external backup system in place, with two also storing physical backups privately, supplemented by firewalls.

Market & solutions

- Enterprise Resource Planning (ERP) systems are central to the digital toolset of participating companies and are crucial for day-to-day operations, representing a significant cybersecurity risk.
- Trust in IT service providers is relatively higher, though constrained by a lack of knowledge to assess service quality and competence.
- Relationships with IT partners are sometimes seen as a burdensome dependency. Considerable time and resources have been invested in customizing solutions, resulting in technical debt. Changing service providers is complicated by the fear of losing previous work and reallocating resources.
- Participants prefer a single point of contact responsible for all solutions in the event of a problem, but question their ability to judge whether services meet their real needs or are driven solely by commercial considerations.

Incident

- Only one of the participants experienced an incident with very limited consequences, which reinforced the feeling of confidence in cybersecurity capabilities.
- The other three participants had not experienced an incident in their current company.

Regulations

- GDPR stipulations are often proactively incorporated into business materials.

Certification

- Cybersecurity certifications are seen as cumbersome and detached from the reality of SMEs. Achieving these certifications may focus more on obtaining the 'stamp of approval' rather than effectively integrating and applying the knowledge—a sentiment also true for legal requirements like GDPR compliance.

5 – Conclusion

This comprehensive market study sheds light on the cybersecurity challenges and opportunities facing SMEs in Luxembourg's rapidly evolving digital landscape. The study underscores the growing importance of robust cybersecurity measures for SMEs, highlighting their vulnerability to a broad spectrum of threats ranging from cyberattacks to regulatory compliance issues. The findings emphasize the need for a multi-faceted approach that encompasses technological, regulatory, educational, and collaborative strategies. We have compiled the key findings of the study to outline the cybersecurity needs of SMEs and also to propose a series of recommendations aimed at filling existing gaps, which are detailed in the subsequent sections below.

5.1 – Aligning research hypotheses with key findings

Political & legal factors:

- **Trends:** Both focus group and survey results indicate a general awareness and incorporation of legal frameworks like GDPR in SME operations. However, there's a sentiment that cybersecurity certifications, while acknowledged, are often seen as cumbersome and not always directly applicable to SME realities.
- **Analysis:** The perception of certificates and legal statuses among SMEs seems to align with the hypothesis that these are only attractive if they present a clear legal requirement or offer a competitive advantage. This suggests a need for more tailored legal frameworks and certifications that resonate with the diverse nature of SMEs.

Economic factors:

- **Trends:** The focus group findings show a growing allocation of budgets to cybersecurity, though often as a part of broader IT budgets. In contrast, the survey results reveal a significant number of SMEs lacking a dedicated cybersecurity budget.
- **Analysis:** This disparity supports the hypothesis that the cost of cybersecurity services can be a barrier. Furthermore, the extensive use of digital tools and platforms, as indicated in the survey, aligns with the hypothesis that higher technology use increases exposure to cyber threats.

Social factors:

- **Trends:** Both sources highlight varying levels of cybersecurity awareness and training, with the focus group emphasizing informal practices and the survey showing a mix of formal and informal cybersecurity education.
- **Analysis**: The data supports the hypothesis that employee digital practices can introduce new risks, especially in the absence of formal training. Additionally, the varying levels of confidence in managing cyber incidents, particularly among leaders, reflect the hypothesis that risk perception is often based on the leaders'

understanding.

Technological factors:

- **Trends:** The focus group discussions and survey responses both underscore the integration of various digital technologies and cybersecurity solutions in SME operations.
- **Analysis:** This widespread adoption of technology supports the hypothesis that technological integration is a driver for developing a cybersecurity culture. However, the sentiment that cybersecurity services are not always tailored to SME needs, as evidenced by the focus group, affirms the hypothesis that available services might not meet all SME requirements. This gap suggests a need for more customized cybersecurity solutions for SMEs, potentially supported by public actors.

The combined insights from the focus group and survey indicate that while Luxembourg's SMEs are increasingly aware of and engaged with cybersecurity, there are gaps in training, budget allocation, and the applicability of existing solutions and certifications to their diverse needs. This analysis underscores the necessity for more nuanced, flexible, and SME-focused approaches in cybersecurity strategies, policies, and services within Luxembourg.

5.2 – Perceived needs of Luxembourg SMEs:

Cybersecurity as a key driver for digitization: Recognizing the interdependence of cybersecurity and the digitization of SMEs is crucial. As SMEs increasingly rely on digital tools and platforms to enhance their operations and reach, they inadvertently expose themselves to various cyber threats. Cybersecurity, therefore, becomes a foundational element in their digital transformation journey.

Action points:

- Prioritize cybersecurity as a fundamental aspect of SME digitization programs and strategies.
- Launch awareness campaigns to underline the importance of cybersecurity in achieving successful and safe digital transformation for SMEs.
- Collaborate with or regulate technology providers to ensure that as they develop digital tools for SMEs, they integrate strong cybersecurity measures from the onset.

Cost-effective, automated, tailored solutions: There is a lack of affordable and tailored cybersecurity solutions specifically designed for SMEs with limited resources. Off-the-shelf solutions might not address the unique needs and constraints of smaller businesses.

Action points:

- Encourage the development of cost-effective cybersecurity tools and services customized for SMEs.
- Support innovation in the cybersecurity sector to create adaptable solutions that cater to different industries and sizes.
- Utilize open-source AI solutions, which can be overseen nationally to improve the individual abilities of SMEs to scan, identify, and alert both end-users and CSIRT regarding concerns.
- Conduct an assessment to identify blind spots where insufficiently digitized or small companies are not adequately covered by cybersecurity solutions.

Budget considerations for cybersecurity: Financial constraints often dictate the direction of organizational strategies, especially for SMEs. Budgeting plays a pivotal role in determining the extent and nature of cybersecurity measures an organization can implement. Without adequate budgeting for cybersecurity, SMEs risk being under-protected, leaving them vulnerable.

Action points:

- Raise awareness among SME leaders about the long-term cost benefits of investing in cybersecurity, highlighting the potential financial ramifications of a cyber breach.
- Provide financial incentives or subsidies to SMEs to support the adoption of comprehensive cybersecurity solutions.
- Organize workshops and seminars to guide SMEs on effective budget allocation for cybersecurity, emphasizing its criticality in the contemporary digital business environment.

Persistent cybersecurity skills gap: SMEs often lack the in-house skills to effectively manage and implement cybersecurity measures, and to assess their needs for new solutions. The result is a gap between awareness and implementation as well as a feeling of “blind trust” in the solution providers.

Action points:

- Emphasize the need for regular training and awareness programs tailored to the needs of SMEs, encouraging employee upskilling and reskilling, and ensuring that they are delivered on an annual basis.
- Use trusted intermediaries, such as professional organizations and government agencies, to help bring SMEs into contact with cybersecurity companies according to their needs.
- Encourage partnerships between larger cybersecurity firms and SMEs to educate their customers by providing expertise and guidance.

Ensuring compliance for SMEs through supportive platforms: Navigating the complex landscape of cybersecurity regulations, standards, and frameworks is particularly challenging for SMEs. Many are unsure about the specific requirements they need to fulfill.

Action points:

- Simplify and consolidate compliance frameworks to provide clearer guidelines for SMEs.
- Develop online platforms or tools that help SMEs understand and efficiently managing their regulatory responsibilities, thereby transforming regulations into a source of competitive advantage.
- Initiatives such as ALTO[57] (led by the CNPD and NC3) and CORAL[58] (led by ILNAS, ANEC, and LHC/NC3) exemplify the potential of simplifying the regulatory framework with a focus on the needs of SMEs, as well as the development of tools tailored to better serve this audience.

Strengthening supply chain security by engaging non-expert contacts in SMEs: SMEs, often integral to expansive supply chains, are vulnerable to cyber risks emanating from third-party ties and dependencies. More importantly, the main contact in these SMEs is rarely a cybersecurity or IT expert, making effective crisis communication imperative.

Action points:

[57] Common Vulnerabilities and Exposures (CVE), Source: MITRE Corporation, Last Accessed: 26/10/2023, Link: https://cve.mitre.org/

[58] Coral Project, Source: Coral Project, Last Accessed: 26/10/2023, Link: https://coral-project.org/

- Promote supply chain risk assessments and cybersecurity audits to identify potential vulnerabilities such as the Fit4Cybersecurity[59] tool.
- Develop guidelines and best practices for securing third-party relationships, encouraging due diligence and risk mitigation.
- Initiate a centralized directory that lists primary contacts to facilitate seamless communication during cybersecurity breaches, and streamline information sharing about threats and crucial vulnerabilities for the CERT-LU community, emphasizing technical expertise over commercial exploitation.

5.3 – Strategic recommendations for enhancing public initiatives

1. **Incubation and support companies specializing in compliance and automation**: Promote the growth of companies focusing on cybersecurity solutions tailored for SMEs by emphasizing compliance and harnessing open-source LLM technology. This approach ensures cost-effective adaptations to the diverse and intricate SME environments, making otherwise unfeasible solutions profitable.
2. **Educational imperatives in cybersecurity:** Begin cybersecurity education in schools, underscoring its growing importance. Design and support versatile educational programs such as the Digital Learning Hub[60] that range from awareness to technical skills, and are aimed at everyone from students to business leaders, to integrate cybersecurity into a lifelong learning approach to protecting individuals and organizations.
3. **Regulatory simplification advocacy:** Collaborate with regulatory bodies to advocate for streamlined and SME-friendly cybersecurity regulations. Work towards harmonizing national and European standards to simplify compliance efforts. Leverage the work done by the CNPD and the Institut Luxembourgeois de Régulation ILR.
4. **Centralized contact directory for breaches:** Initiate a directory for individuals to contact during cybersecurity incidents, streamlining the flow of crucial threat information within the CERT-LU community[61] and emphasizing knowledge-sharing over commercial goals.
5. **Facilitating SME awareness of their needs with trustworthy intermediaries:** Employ trusted entities, such as professional organizations and government bodies,

[59] Fit4Cybersecurity, Source: NC3 (National Centre for Cybersecurity), Last Accessed: 26/10/2023, Link: https://fit4cybersecurity.nc3.lu/

[60] About Digital Learning Hub, Last Accessed: 08/11/2023, Link: https://dlh.lu/about-us/

[61] CERT-LU, Source: CERT-LU, Last Accessed: 08/11/2023, Link: https://cert.lu/

to connect SMEs with cybersecurity firms tailored to their specific needs. Establish a link between the Cybersecurity Luxembourg ecosystem platform[62] and the Fit4Cybersecurity[63] tool to assess company needs and facilitate connections with local providers of cybersecurity services and products.

6. **Jumpstarting security measures for SMEs through financial aid:** Develop the "Fit4Cybersecurity"[64] program for SMEs with a public-private partnership, backed by the Chamber of Commerce. This program aids SMEs in assessing their IT and cybersecurity needs and enhancing protection. Consider partial subsidies for SMEs' expenses and offer financial incentives to encourage investment in vital cybersecurity technologies and services.

5.4 – To go further

In this report, we've examined the cybersecurity challenges confronting SMEs, but our findings also highlight areas ripe for more in-depth investigation. Starting as an initial foray into Luxembourg's cybersecurity market from the SME lens, this study paves the way for a subsequent, more detailed analysis focusing on service providers. Another point raised by our research is the perceived imbalance in cybersecurity investments versus their tangible returns. This insight naturally leads to another critical area for exploration - the cybersecurity talent market. There is a clear need to understand and address the disconnect between the availability of skilled professionals and the industry's needs. Simultaneously, it's essential to anticipate and understand the impact of emerging technologies, particularly AI. These advancements hold the potential to significantly alter the cybersecurity landscape in the foreseeable future, with implications both beneficial and adverse.

[62] Private sector dashboard, Source: CERT-LU, Last Accessed: 08/11/2023, Link: https://www.cybersecurity.lu/ecosystem?tab=private-sector

[63] Fit4Cybersecurity online survey, Source: NC3, Last Accessed: 08/11/2023, Link: https://fit4cybersecurity.nc3.lu/

[64] Poser les fondations d'une "Data-driven Economy" compétitive et innovante, Source: Luxembourg Chamber of Commerce, Last Accessed: 26/10/2023, Link: https://www.cc.lu/toute-linformation/publications/detail/elections-2023-poser-les-fondations-dune-data-driven-economy-competitive-et-innovante?tx_ccpublications_publications%5Bpage%5D=1&cHash=efcc92a278e9b20161b9394843071dde

nc3 Cybersecurity Observatory

How to quote the report:

"NC3 Observatory - Cybersecurity Market Study - December 2023"

Download it here:

https://observatory.nc3.lu/market-intelligence-library/

Published by

nc3.lu
National Cybersecurity
Competence Center
LUXEMBOURG

December 2023