CyberHubs

Cybersecurity Skills Needs Analysis report Estonia.

Co-funded by
the European Union

About CyberHubs

The European Network of Cybersecurity Skills Hubs (CyberHubs) is a 3-year project aiming to enhance the cybersecurity skills ecosystem in Europe. It will establish a network of seven Cybersecurity Skills Hubs in Belgium, Estonia, Greece, Hungary, Lithuania, Slovenia, and Spain, which will promote the development of digital skills in cybersecurity and support the development of a skilled cybersecurity workforce.

Expected results of the project include the establishment of a sustainable European Network of Cybersecurity Skills Hubs, the development of national cybersecurity skills strategies, the creation of innovative cybersecurity solutions through the Hackathon and the establishment of long-term partnerships and collaboration with the wider cybersecurity ecosystem.

Project consortium

The CyberHubs consortium brings together 21 full partners spanning 11 European Member States and 3 associated partners.

Full partners

DIGITALEUROPE | ADECCO FORMAZIONE SRL | AGORIA | AMETIC | Athens University of Economics and Business | Breyer Publico SL | Cyber Ireland | EIT Digital | GZS/CCIS | HOWEST | INFOBALT | ITL Estonia | IVSZ | Kaunas University of Technology | NUMEUM | SEPE | Solvay Brussels School of Economics and Management | Tallinn University of Technology | Universidad Internacional de La Rioja (UNIR) | Ludovika University of Public Service (NKE) | UNIVERZA V MARIBORU

Associated partners

Association of Applied Research in IT (AAVIT) | Digital Technology Skills (DTSL) | IT Ukraine

Legal Disclaimer

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the European Union

Copyright © 2024 by CyberHubs

All rights reserved.

Cybersecurity Skills Needs Analysis report - Estonia, 2024, final version.

Deliverable D2.1: "Cybersecurity Skills mismatches analysis"

Authors: Birgy Lorenz (Tallinn University of Technology)

Editors/Reviewers: 0.1 Grete Soares de Camargo (Estonian Association of Information Technology and Telecommunications) 0.2 Jüri Jõema (Estonian Association of Information Technology and Telecommunications), Anu Baum (TalTech) 0.3 Anto Veldre (Cybernetica), Adrian Nicholas Venables (Tallinn University of Technology), Grete Soares de Camargo (Estonian Association of Information Technology and Telecommunications)

Revision History			
Version	**Date**	**Modified by**	**Version**
0.1	13/09/2024	Birgy Lorenz (Tallinn University of Technology)	Draft version 1.0
0.2	29/09/2024	Birgy Lorenz (Tallinn University of Technology)	Draft version 2.0
0.3	02/10/2024	Marie Montaldo (DIGITALEUROPE)	Review of the full report and comments
0.4	27/10/2024	Birgy Lorenz (Tallinn University of Technology)	Draft version 3.0
0.5	27/10/2024	Marie Montaldo (DIGITALEUROPE)	Formatting inspection and changes
1	28/10/2024	Birgy Lorenz (Tallinn University of Technology)	Final version

Table of contents

Executive Summary 7
1 Introduction 10
1.1 Cybersecurity skills in Estonia 10
1.2 Research approach 10
1.3 Reading guide 11
2 Desk research (demand) 12
2.1 Data collection 12
2.2 Overview of the national context 12
2.2.1 Politics and agencies 12
2.2.2 Laws and regulations 14
2.2.3 Market 15
2.2.4 Society 15
2.2.5 Technology 16
2.3 Literature, Labour market reports and databases 17
2.3.1 Roles 17
2.3.2 Skills 18
2.4 Conclusions 19
3 Questionnaire 21
3.1 Data collection 21
3.2 Results 21
3.2.1 Overall results 22
3.2.1.1 Roles and responsibilities 22
3.2.1.2 Skills analysis 23
3.2.1.3 Hiring and upskilling staff 27
3.2.2 Cybersecurity roles cybersecurity service providers 29
3.2.2.1 Analysis of Cybersecurity Skills, Training Needs, and Hiring Criteria 30
3.2.2.2 Training Approaches and Importance 30
3.2.2.3 Hiring Criteria 31
3.2.2.4 Challenges in Training Cybersecurity Personnel 31
3.2.3 Companies with the Need of In-house Cybersecurity Professionals 31
3.2.3.1 Training Approaches and Importance 32
3.2.3.2 Challenges in Training 32
3.2.4 Comparison: Cybersecurity Service Providers vs. Cybersecurity Service Users and key takeaways 32
3.3 Conclusions 34
4 Job vacancy analysis 34
4.1 Data collection 34
4.1.1.1 Major Job Portals in Estonia 35

4.1.1.2 Professional and Networking Platforms 35
4.1.1.3 General Keywords 35
4.2 Results 37
4.2.1.1 Analysis of the Scraping-EU Level Dataset 37
4.2.1.2 Estonian local scraping by hand Dataset 38
4.3 Conclusions 41
5 Desk research (supply) 42
5.1 Data collection 42
5.2 Results 42
5.3 Conclusions 43
6 Expert panel 45
6.1 Data collection 45
6.2 Results 45
6.2.1 Cybersecurity roles 45
6.2.2 Skills for cybersecurity professionals 46
6.2.3 Training of cybersecurity professionals 48
6.3 Conclusions 50
7 Conclusions 51
7.1 Cybersecurity roles 51
7.2 Skills for cybersecurity professionals 52
7.3 Education and training of cybersecurity professionals 53
8 References 55

List of Figures

Figure 1: Needs for Roles in the Company 22
Figure 2: Cybersecurity Skills needed for Cybersecurity Role, % who said “yes” at the survey 23
Figure 3: IT-skills needed for Cybersecurity Roles, % who said “yes” at the survey 24
Figure 4: Organizational skills needed for Cybersecurity Roles, % who said “yes” at the survey 25
Figure 5: Transferable Skills needed for Cybersecurity Roles, % who said “yes” at the survey 26
Figure 6: What Is Important when you hire new staff? % who said “yes” at the survey 27
Figure 7: How do you hire and upskill your staff? % who said “yes” at the survey 28

List of Tables

Table 1: Data collection in numbers 12
Table 2: Key differences of strategies of cybersecurity Service Providers and Need of In-house Cybersecurity Professionals 34

Executive Summary

Introduction

The CyberHubs project aims to strengthen Europe's cybersecurity workforce by creating a network of 7 Cybersecurity Skills Hubs in Belgium, Estonia, Greece, Hungary, Lithuania, Slovenia, and Spain. Coordinated by DIGITALEUROPE, the project includes 21 partners from 11 EU Member States, focused on improving cybersecurity skills and fostering digital expertise.

The project focuses on analysing cybersecurity skills gaps, developing national cybersecurity strategies, organising a European Cybersecurity Hackathon, and fostering collaboration between education and industry. Stakeholders, including students, professionals, and public organisations, will gain access to cybersecurity resources and job opportunities.

The cybersecurity sector in Estonia remains at the forefront of global digital defence, leveraging its pioneering foundation in the field. Estonia is recognized as the advanced cyber security country in Europe, with unique expertise in research, development, and management of cyber security solutions. Estonia ranked 3rd on the global scale in the Global Cybersecurity Index (GCI) 2020 (Estonia.ee, 2021) and 2024 5th (ITU; 2024). However, the rapidly changing nature of cybersecurity poses ongoing challenges, and continuous efforts are required to ensure preparedness and protection against cyber threats.

The current state of cybersecurity in Estonia is a matter of concern of phishing, fraud and service interruption. Service interruption attacks has been increased annually due to Russian-Ukraine war (Information System Authority, 2024a). The cybersecurity workforce in Estonia faces a critical skills gap. Cyber Security workforce is expected to grow a need to ~200 specialists annually due to implementation of Estonian Information Security Standard (Praxis, 2019; Kutsekoda, 2022a; 2022b; 2022c).

Estonia as a country emphasises cyber norms, international cooperation, information sharing, defence, and risk management as tools for deterrence against cyber threats. Estonia also defines obligations for vital infrastructure companies and relevant government institutions and promotes collaboration with the private sector to strengthen cyber security.

Objective and Approach

The Needs Analysis report aims to uncover the critical needs for cybersecurity skills and professional roles in Estonia, considering the country's cybersecurity ecosystem status and its opportunities and peculiarities. It will also feed the development of a country-specific Cybersecurity Skills Strategy with the information on the current and future demand for cybersecurity skills and roles and on the current supply of cybersecurity learning offering.

This study adopts a multi-method approach whereby both primary and secondary data collection is used as input for the analysis. This approach includes: i) a (demand) desk research to gain insight on potentially relevant cybersecurity roles and skills with a study of the existing literature (scientific papers, labour market reports, and labour market databases) and a job vacancy analysis, ii) a questionnaire to collect data from industry and other relevant actors on the current and future needs for cybersecurity professional roles and skills, iii) a (supply) desk research to get an overview of the current cybersecurity learning offering, and iv) an expert panel to explore future situations and validate the results from the quantitative data collection. This methodological approach uses European frameworks, like the European Cybersecurity Skills Framework (ECSF) and other relevant frameworks, as a foundation to specify the main cybersecurity missions, tasks and skills needed in a professional cybersecurity context, making it a valuable reference for profiling skills and knowledge needed by cybersecurity professionals.

Results

Estonia excels in cybersecurity leadership but must address the workforce shortage and overall citizenship awareness, due to geographical situation. Collaboration across sectors and targeted skill development are essential to maintain its digital defence capabilities. Demand for cybersecurity professionals is growing rapidly, yet Estonia's education system only produces a fraction of the required graduates. Efforts to close the gap include national strategies, private sector collaboration, educating commoners but also leaders of the companies and training initiatives for the IT and cybersecurity specialists, though bureaucratic obstacles remain.

- In Estonia Total ICT workforce in 2024 is around 5,1% and Cybersecurity professionals or professionals that needs cybersecurity skills is around 1,1%. Focus is to get more people in positions of Secure Software Development, Cybersecurity Specialists and Incident Responders with skills of Pen-testing, cloud security, secure systems administration as both cyber security service providers and SMEs needs more experts. Also, when looking at the future needs of the cyber security filed emerging topics like AI security needs more attention. Also, special focus of cryptography is noted.
- When looking at need of skills Estonia needs to focus on giving strong basic skills in cybersecurity and IT to the students who study like Cloud Security, Information Systems & Network, Security/Cyber Resiliency, Access Controls/Identity Management, Data Privacy, Enterprise Architecture & Infrastructure Design, System Administration & Integration, Data Analysis, Software Development and Computer Languages, and organisation and transferal skills like Education and Training Delivery & Development, Risk Management, Project Management, Law, Policy and Ethics, Analytical Thinking, Communicating, Willingness to Learn, Problem Solving. Other needed skills seem to be left to the industry to figure them out through specialized training, upskilling people inside the company, coaching or other.
- Estonian situation is common to smaller country - most companies (120,000) are SMEs, most with fewer than 10 employees. This severely limits the possibility of hiring any in-house cybersecurity professionals. As a result, outsourcing methods and related trust issues hold greater significance here than the EU average. So, the current job market shows more job offerings for Secure Software Development than Cybersecurity Implementer and CISO/Leadership Positions roles, that also seems to pop out the most. At the offering the people are asked to show their real-life experiences rather than official degree. Also, as companies often need generalists rather than specialists, that one can adapt to various roles within an organisation and then, if needed receive special training. Companies also look only to hire specialist who has real job experiences, and this shows issues with high entry to the filed for the university graduates that have not got practice or have not worked throughout the study.
- Estonia has made notable strides in incorporating cybersecurity education into its national curriculum, vocational training, and higher education, providing various entry points for skill development. However, universities primarily offer foundational cybersecurity knowledge in English, and advanced specializations are limited. Master's level programs like the Cyber Defense track provide deeper knowledge but are still insufficient to meet the rising demand for skilled professionals. Challenges remain, including a shortage of educators, limited specialized coursework, and a language barrier due to Estonia's unique linguistic structure. The reliance on English for instruction and research has hindered the development of Estonian cybersecurity terminology, complicating training and industry communication. Additionally, universities in smaller countries like Estonia struggle with sustainability issues, especially considering reduced international student intake due to global security concerns and pandemic impacts. To address these gaps, increased cooperation between government, academia, and industry, along with targeted outreach to young learners, will be vital for developing a robust pool of cybersecurity talent.

Conclusions

- Results showcase why it is needed to boost Europe's cybersecurity workforce and digital transformation in every country. Key results are also valuable for developing a sustainable network of Cybersecurity Skills Hubs, national strategies, innovative cybersecurity solutions, and strong partnerships in the EU.
- Main takeaways are:
    - Estonia is a leader in cybersecurity but faces significant workforce shortages and lacks widespread public cybersecurity awareness, which is especially critical given its geographic and geopolitical

context. Rapidly increasing demand for cybersecurity professionals outstrips the capacity of Estonia's education system to supply qualified graduates.

- The focus is on developing skills for roles like Secure Software Development, Cybersecurity Specialists, and Incident Responders, with an emphasis on areas like AI security and cryptography. Basic skills in cloud security, identity management, data privacy, and enterprise architecture are also needed, yet many specialized skills are left for companies to provide through in-house training.
- Most Estonian companies are SMEs with limited resources to hire dedicated cybersecurity professionals, increasing reliance on outsourcing and raising trust-related challenges. Employers are particularly interested in real-world experience over formal degrees, making industry entry difficult for recent graduates without hands-on experience.
- While Estonia has integrated cybersecurity education into its national curriculum and vocational training, offerings are mostly foundational and in English, limiting the development of an Estonian cybersecurity terminology. To overcome these educational and linguistic challenges, Estonia needs enhanced government, industry, and academic collaboration to support long-term talent growth and sector resilience.

1 Introduction

1.1 Cybersecurity skills in Estonia

In recent years, Estonia has experienced significant developments in its cybersecurity landscape. The country, widely regarded as a global leader in digital defence, continues to face increasing cyber threats like phishing, fraud and service interruption. The country ranks 5th globally in the Global Cybersecurity Index according to the International Telecommunication Union and National Security Index (ITU; 2024; NCSI, 2024), underscoring its leadership in the field. Estonia's strategic collaboration with NATO and the development of national cybersecurity frameworks ensure it remains prepared for evolving threats. However, the rapid pace of technological change continues to challenge Estonia's defence capabilities, with a particular need for skilled cybersecurity professionals.

The current state of cybersecurity in Estonia is a matter of concern of phishing, fraud and service interruption. The cybersecurity workforce in Estonia faces a critical skills gap. Demand for professionals, especially in roles such as cybersecurity implementers, incident responders, and penetration testers, is projected to grow by 1.5 times by 2027. Yet, current educational and training systems are struggling to meet this demand, as Estonia produces only 735 graduates annually against the required 2,600 new specialists in the IT sector and even less in cyber security (Kutsekoda, 2022a; 2022b; 2022c). Cyber Security workforce is expected to grow 200 annually in next year's due to implementation of Estonian Information Security Standard (Praxis, 2019; Kutsekoda, 2022a).

Efforts to close this gap include national cybersecurity strategies, collaboration with private sectors, and advanced training initiatives aimed at reskilling existing professionals and attracting international talent. However, bureaucratic hurdles and the high demand for specialised roles across Europe pose additional challenges.

Estonia continues to emphasise cybersecurity education at all levels, offering specialised university programs and promoting digital literacy among students. Additionally, upskilling initiatives and real-world training experiences are vital to preparing the next generation of cybersecurity professionals.

In summary, while Estonia excels in its cybersecurity capabilities and frameworks, addressing the skills mismatch is critical to sustaining its leadership. Enhanced collaboration between government, educational institutions, and private sectors, alongside targeted investments in skill development and recruitment, will be key to securing the future of Estonia's cybersecurity infrastructure.

1.2 Research approach

The aim of the research is to improve cybersecurity education and workforce development by identifying the gaps between current supply and future demand for cybersecurity professionals. Focus is on Estonian-specific cybersecurity skills mismatches, forecasting future demand.

This research uses a multi-method approach to analyse cybersecurity skills mismatches. Data collection methods include desk research on current and future labour market needs, job vacancy scraping, questionnaires to organisations, and expert panel discussions. The methodology ensures a comprehensive analysis of both demand and supply, focusing on national-level cybersecurity skills gaps to inform strategic development.

Key tasks include:

1. Identifying discrepancies between the skills professionals possess and those needed by the labour market.
2. Using desk research, questionnaires, job vacancy analysis, and expert panels to collect data on current and future needs.
3. Mapping the current supply of education and training programs.

4. Comparing demand and supply to identify critical skills shortages.

1.3 Reading guide

This document provides a detailed analysis of cybersecurity needs and skills mismatches in Estonia, organized into several key sections:

- An overview of the cybersecurity landscape in Estonia, including the current state of cyber threats, national strategies, and the demand for cybersecurity professionals.
- A description of the methodology used, including desk research, job vacancy analysis, expert panel discussions, and data collection techniques such as surveys and interviews.
- Key findings from the data collection, offering insights into the roles, skills, and hiring challenges in the cybersecurity sector. It includes an analysis of the demand for cybersecurity professionals and the training needed to close the skills gap.
- Summarizes the major findings, highlighting the skills mismatch, workforce shortages, and recommendations for improving Estonia's cybersecurity talent pipeline.

2 Desk research (demand)

2.1 Data collection

The data collection process for this study involved multiple methodologies to ensure a comprehensive understanding of the cybersecurity needs in Estonia. This approach was designed to map out the current supply and demand for cybersecurity professionals, assess workforce gaps, and gather expert perspectives on the future of cybersecurity needs in Estonia. The research gathered data from various sources, including academic papers, strategies or regulations, other reports Including also labour market reports, and labour market databases. Additionally, websites were reviewed to provide further insights into Estonia's cybersecurity landscape.

Data collection in numbers	
Literature	22 papers/ articles included in analysis, 6 strategies or regulations, 7 other sources
Labour market desk research	7 labour market reports
Labour market databases	10 labour market databases

Table 1: Data collection in numbers

2.2 Overview of the national context

Overall, Estonia has a well-established organisational framework for cybersecurity at the national level, with key actors and organisations collaborating to ensure cyber resilience.

2.2.1 Politics and agencies

The "Cybersecurity Strategy 2024-2030" outlines Estonia's national cybersecurity strategy for the years 2024 to 2030. The key focus of the strategy is on strengthening Estonia's cybersecurity framework in response to evolving global threats, particularly in the context of increasing cybercrime, ransomware attacks, and geopolitical tensions, such as those arising from Russia's war in Ukraine.

International Telecommunication Union (ITU) (2024b) ranks Estonia organization and cooperation measures 20 out of 20. Also, they see potential growth in a technical measures and capacity development measures. Estonian tier performance is Role-modelling. NSCI rates at the same time Estonian Policy worth 60/100; Global Contribution 100/100; Research and Development 50/100; Fight to Cybercrime (Police) 100/100 and Military defence level 67/100 (NCSI, 2024).

Key Ideas and Focus:

- The strategy focuses on four primary areas: managing national cybersecurity development, enhancing societal resilience, strengthening incident monitoring and prevention, and fostering a secure cyber environment both in Estonia and globally (e-Estonia, 2021; 2023).
- Estonia faces increasing cyber threats due to its highly digitalized society. The document highlights the importance of international cooperation, particularly with NATO and the EU, to address these challenges.
- Cyber resilience: The strategy emphasises societal preparedness, urging public and private sectors to strengthen cybersecurity measures that are needed to function as digital/information society. A focus is placed on preventing attacks on critical infrastructure and raising awareness among citizens, businesses, and government entities about cyber threats (Valitsus, 2021).
- Incident response and prevention: A key priority is improving real-time monitoring and detection of cyber incidents, with the goal of minimising damage and ensuring rapid recovery from attacks.

- International cooperation: Estonia aims to lead and cooperate on international initiatives, particularly within the EU and NATO, to enhance cybersecurity on a broader scale.
- Education and workforce development: The strategy addresses the need for developing the cybersecurity workforce through education and targeted initiatives, especially to close the skills gap in critical areas.
- Emerging technologies: The document highlights challenges related to technological advancements like AI, quantum computing, and IoT, stressing the importance of developing resilient cybersecurity frameworks that evolve with these technologies. (Pernik, 2021; Kohler, 2020).

The current situation of cybersecurity in Estonia can be summed up as follows:

- Geopolitical tensions have impacted the cybersecurity landscape in Estonia, as seen in the recurrence of DDoS attacks, but also raise of other attacks of phishing. Example, Estonian Information System Authority (RIA) report in 2024 was listed 3314 incidents (out of that 1722 was Phishing, 456 Fraud, 312 Distributed Denial-of-Service (DDoS) (Information System Authority, 2024a)); In 2023 was listed 2672 incidents (out of that 1206 Phishing, 344 DDoS, 236 taking over user accounts) (Information System Authority, 2023)); In 2022 was listed 2237 incidents (out of that 775 was Phishing, 262 Malicious redirect, 254 Distributed Denial-of-Service (DDoS) (Information System Authority, 2022)); In 2021 was listed 2772 incidents (out of that 766 was Botnet, 711 Phishing, 330 Malware (DDoS) (Information System Authority, 2021)); 2019 Incidents list Botnet 55% and Phishing 18.5% and Distributed Denial-of-Service (DDoS) 6% as the main challenges (Information System Authority, 2020a; 2020b)). Looking at the timeline 2017-2024, at year 2018 had most incidents with an impact (3473), but 2023-2024 shows an 32% increase from year 2021.

- Estonia's role in the development of NATO's cyber defence policy has also been exemplary in helping to develop current cyberspace concepts for defending NATO (Laasmäe, 2022). Example NATO CCDCOE is situated in Estonia, and they help to organize training events.
- The Cyber Security Strategy 2024-2030, 2019-2022, 2014-2017 (Ministry of Economic Affairs and Communication, 2014; 2018; 2024) etc. has served as the foundational document for planning Estonia's cyber security and is part of its broader security strategy. In 2008, Estonia released its first national strategy document focused on cybersecurity, recognizing its interdisciplinary nature and the need for comprehensive measures. Now Estonia's Information Security standard (E-ITS), is mandatory for approximately 3,500 organisations, including the Estonian Information System Authority (RIA). This standard Is mandatory If the institution has not already implemented ISO27001 (Information System Authority, 2024c).
- Estonia has implemented several measures and initiatives to combat cyber threats. The country's Red Team, known as the RIA, conducts sophisticated simulations to test and enhance the security of information systems, including phishing emails and physical penetration testing. The division of cyber security tasks and responsibilities between different agencies emphasising the need for clear mandates and competence. Effective communication to a local and global audience is showcased as a key aspect of cybersecurity in Estonia. The Estonian Internal Security Service, known as KaPo, is as responsible for detecting and preventing cyber threats, particularly those arising from cyber intelligence, as well RIA CERT and Estonian Foreign Intelligence Service and others (Cyber/Ireland, 2024).
- There are also several initiatives to upskill IT-personnel skill sets in cyber security, also how to involve students to take interest in cyber security through testing, competitions and summer camps that are mentioned later in a paragraph about education and society (e-Estonia, 2021; 2023).

Some examples of agencies and their initiatives:

Until 2024 The Ministry of Economic Affairs and Communications was responsible for coordinating cybersecurity measures, and the Information System Authority provided guidance and support to companies and individuals. Currently 2024, due to changes in governance responsibility, cyber security matters are transferring into the responsibility of the Ministry of Justic.

The National Cyber Security Centre of Estonia and the Cyber Command headquarters also play significant roles in cybersecurity. Companies and individuals can turn to the CERT-EE for reporting incidents and seeking assistance. Enabling the military industry to participate in EU defence initiatives like the European Defence Fund and European Defence Industrial Development Plan is another step (Defence Industry and Space, 2024).

National Cyber Security Centre and EAS/Kredex distributes support for mapping and increasing the level of cyber security to small and medium-sized companies in several sectors during a pilot project (19.4 million Euros) (EAS, 2022). Currently effectiveness of the support Is analysed by PwC and TalTech.

The Estonian Information Security Association (EISA) promotes university-business-government collaboration. The work they do emphasises cooperation based on relevant capabilities with an administrative support structure for cross-sectorial participation in bidding on international contracts and competition to establish the preconditions for export and research financing.

The organisations around cybersecurity at the Estonian national level are focused on protecting the country's digital infrastructure and ensuring secure communication between citizens and the government. The main entity responsible for this is the Cyber Defence Unit of the Estonian Defence League, which consists of experts in the field who contribute to the effort (CCDCOE, 2013).

To help foster the startup ecosystem - Startup Estonia initiative works closely with various ministries and stakeholders to bridge different sectors with the startup community, promoting innovation and entrepreneurial growth. Startup Estonia has identified four key focus areas for systematic support: Enhancing the ecosystem for startups, including infrastructure, regulations, and support network; Supporting startups involved in advanced technologies such as cybersecurity, AI, and data science, which are crucial for future technological development; Attracting and retaining international talent to strengthen Estonia’s innovation landscape; Promoting entrepreneurship across all regions of Estonia to ensure balanced economic growth. The initiative is instrumental in supporting Estonia's reputation as a leader in deep tech, particularly in cybersecurity, and in driving collaboration between the private sector, government, and international stakeholders (Startup Estonia, 2024; 2023).

Also, we can make note of The Tallinn Digital Summit, as it is an annual high-level event initiated by the Prime Minister of Estonia and has offered open debate already over 20 years. It gathers top policymakers, thought leaders, entrepreneurs, and the tech community to highlight the importance of digital transformation and address its impact on economies, societies, and nations and there is always some focus of cyber security.

Other agencies are listed at the Cybersecurity Strategy 2024-2030 (Ministry of Economic Affairs and Communication, 2024).

2.2.2 Laws and regulations

Estonia takes proactive measures to strengthen cyber security and protect its critical infrastructure and people. International Telecommunication Union (ITU) (2024b) ranks Estonia legal measures 20 out of 20. NSCI rates at the same time Cybersecurity Enablers 83/100, Protection of Personal Data 100/100 (NCSI, 2024).

The regulatory landscape of cyber security in Estonia encompasses both national legislation and European Union (EU) legislation. Estonia has specific national legislation in place, for example the Cyber Security Act, to address cyber security issues and strengthen measures in the country.

The Cyber Security Strategies 2024-2030, also former 2019-2022, 2014-2017 etc. has served as the foundational document for planning Estonia's cyber security and is part of its broader security strategy. In 2008, Estonia released its first national strategy document focused on cybersecurity, recognizing its interdisciplinary nature and the need for comprehensive measures.

Additionally, Estonia adheres to EU legislation and aligns its national legislation with EU directives, legislation and regulations to ensure compliance with EU. The implementation of EU legislation is handled through coordination and cooperation between Estonia and the EU. Estonian law is in line with EU law. Various laws and acts, including the Penal Code, Constitution of Estonia, Personal Data Protection Act, Network and Information Security Directive (2) and the already mentioned Cybersecurity Act, contribute to the comprehensive legal framework for cyber security in Estonia (Riigiteataja 2019; 2022).

To enhance information security, Estonia has established the Information Security Standard E-ITS, which promotes best practices and guidelines for ensuring the security of information systems (Information System Authority, 2024c).

The report of Estonia at CyberSecPro - D2.1 states: *Estonia's cybersecurity strategy, Cybersecurity Strategy - Republic of Estonia (EE), was implemented already in 2019 and it involved Estonia's civilian, military, public sector, critical infrastructure service providers, sectoral entrepreneurs, and academia. The next revised plans address 13 of the 15 ENISA self-assessment strategic goals: Cybercrime security and privacy balance; Citizen awareness; Critical information infrastructure protection; National cyber contingency plans; International cooperation; Incident response capability; Institutionalised public agency cooperation; Baseline security requirements; Incident reporting mechanisms; R&D; Cybersecurity exercises; Training and education.*

2.2.3 Market

Estonia is a recognized leader in cybersecurity in Europe, known for its expertise in the research, development, and delivery of cybersecurity solutions. The country is home to several internationally recognized cybersecurity firms, such as Malwarebytes, Cybernetica, CybExer Technologies, Clarified Security, Guardtime, Nortal, Andmevara, RangeForce and other offering solutions ranging from malware protection and digital identity to cybersecurity training. Also, the presence of world-leading companies in the country highlights the importance and attractiveness of Estonia as a cybersecurity hub. Estonia's core strengths include secure digital identity, cryptography, data integrity, and cybersecurity skills and training, making it a prominent player in the cybersecurity field (Ministry of Foreign Affairs of Estonia, 2024). Praxis 2019 overview of the job market report lists several other organizations who provide services in compliance, data protection policies; detection and prevention; network security; identity management, authentication; training and awareness; endpoint security; incident response and forensics; web security; cyber posture (Praxis, 2019).

The cybersecurity market in Estonia is projected to experience significant growth in the coming years. According to Statista, it is estimated to grow by 8.12% between 2024 and 2029, resulting in a market volume of US$108.00m (€97,800,000.00 EUR) in 2029. The average Spend per Employee in the Cybersecurity market is projected to reach US$96.88 (87,9 EUR) in 2024. Additionally, the Data Security market in Estonia is expected to grow by 11.46% during the same period, leading to a market volume of US$4.80m (4,350,000.00 EUR) in 2029. The average Spend per Employee in the Data Security market is projected to reach US$3.70 (3,7 EUR) in 2024 (Statista, 2024a; 2024b).

In addition, due to the elevated international and local interest in the cybersecurity services provided by the members of Estonian Association of Information Technology and Telecommunications (ITL) a CyberTech sub-cluster has recently been formed. The CyberTech cluster is made up of more than 20 member companies that offer cybersecurity related products or services and are interested in collaborating with other similar companies. The principal aim of the CyberTech cluster is to support the export of cybersecurity solutions, as well as grow awareness in Estonia (ITL, 2024; ITL, 2022). The review of 48 Estonian cybersecurity firms indicates that their services fall into three main categories: Cyber Prevention/Protection (38% of firms), Cyber Risk Analytics/Consulting/Training (31%), and Identity Verification (31%). Most companies leverage advanced digital technologies, including AI, machine learning, big data, cloud computing, cryptography, and virtual reality (see the questionnaire).

2.2.4 Society

Estonian society is characterised by its diverse demographic composition, educational attainment, and high level of digital proficiency among its citizens. Most of the population in Estonia is made up of ethnic Estonians, comprising 69.1% of the population, followed by Russians at 23.7%, Ukrainians at 2.1%, and other ethnic groups accounting for 4.6%. Notably, about two-thirds of the population are ethnic Estonians, while Russians represent the most significant minority, comprising approximately one-fourth of the citizenry. No other EU nation has had to integrate such many people from foreign cultures and backgrounds over the past 80 years, which brings specific concerns in cybersecurity. This situation, as highlighted by Estonian Internal Security Service annual reports, incurs additional costs—such as translating materials into Russian and navigating trust models that differ due to hierarchical cultural norms. Additionally, each national culture has its own ethical framework; also Estonia continue to face challenges with the distinct ethical perspectives rooted in

Eastern European cultural backgrounds. Also there is an issue with translation machines and web-based service platforms significantly influence the demographic composition, including cultural, religious, and folk traditions. This shift affects the way communities interact with and maintain their cultural identities, as these technologies often promote a more homogenized or universal approach to information and services, impacting traditional structures and values.

In terms of educational attainment, secondary education is the highest level for 42.9% of the population aged 15 and over, while 37.1% have attained a higher education level. Additionally, 20% of the population has basic education or less. However, when looking specifically at the 25–64-year-old age group, 42% have tertiary attainment, which is slightly lower than those with upper secondary or post-secondary non-tertiary attainment. In 2021, 43.2% of Estonians between the ages of 25 and 34 held a university degree, surpassing the EU average of 41.2%. Furthermore, in terms of enrolment, 40% of 15–19-year-olds are enrolled in general upper secondary education, while 15% are enrolled in vocational upper secondary education (Education Estonia, n/a; European Commission, 2020; OECD, 2023).

Estonia has become home to some of the world's most well-known tech startups, showcasing its innovation in the digital realm. Estonia has built a robust system of digital infrastructure, making almost all its government services available online to its citizens and residents. The concept of a digital citizen lies at the core of Estonia's digitization efforts, where individuals access both public and private services through a digital platform. The country's leaders emphasise how digitalization is reflected in its education system, with all schools utilising the "e-school" system, highlighting the importance of digitalization in the governance of the skill system. Estonia ranks high in terms of digital proficiency and is considered one of the most digitally advanced countries in Europe and the world. NSCI rates also Estonian Education 100/100, Threat analysis and awareness raising 100/100 (NCSI, 2024).

For overall awareness of digital hygiene and cybercrime the government has adopted a comprehensive prevention campaign “Be IT-conscious!” to enhance cybersecurity awareness among businesses and citizens (focusing on people 50 and up.). Historically these like awareness like campaign series began as early as pre-2010 and has continued for such an extended period is quite rare in Europe (Information System Authority, 2024d).

2.2.5 Technology

Estonia has a specific focus on cybersecurity and now also artificial intelligence and its implications. International Telecommunication Union (ITU) (2024b) ranks Estonia technical measures 15,3 out of 20. NSCI rates at the same time Estonian Critical Infrastructure 75/100; Cyber Incidents Response 100/100; Cyber Crisis Management 75/100 (NCSI, 2024).

The Estonian government recognizes the importance of investing in technological developments, particularly in the field of cybersecurity (governmental E-Systems and services, digital ID, use of blockchain, AI) (Information System Authority (RIA). (n.d.). It has also made significant investments in research and development, education, and infrastructure to enhance its cyber resilience. The government has also provided tax incentives and promoted an entrepreneurial culture to stimulate technological growth. These measures contribute to the development of a robust technological landscape in Estonia, also to cyber security and emerging technologies (deep tech and example of AI) (Information System Authority, 2024b).

Digital resources are extensively used in different sectors in Estonia. The increasing reliance on technology necessitates a strong focus on cybersecurity to ensure the security of digital resources. These resources are crucial for enhancing professional development in education, supporting student learning, conducting research activities, and improving access to information in various sectors.

Several research papers and articles have been published that explore critical aspects of cybersecurity, including its growing importance, emerging technologies, and management trends. This emphasises the need for continuous research and development to combat emerging threats. The focus is also to analyse the use cases of Artificial Intelligence (AI) in cybersecurity provisioning, highlighting how AI can enhance cybersecurity measures. Additionally, it is important to explore the cybersecurity implications of digital transformation for achieving business resilience.

2.3 Literature, Labour market reports and databases

The search performed for this study involved multiple steps to gather relevant information. In Estonia there Is only few reports on the matter, one of the best is OSKA report (future studies of prognoses of Estonian workforce and skills needs) that combines all the needed data form various sources and as well experts and stakeholders' ideas, providing a comprehensive understanding of workforce needs and educational gaps. There is also EU level report CyberSecPro Project from 2023 about "Cybersecurity Practical Skills Gaps in Europe" and Praxis report about Estonian Cyber security workforce needs form 2019. Also, some help was gained form Fontes 2022, 2023 and Praxis, 2019. These are the base for roles and skills overview.

2.3.1 Roles

Short: Estonia's demand for IT professionals is projected to increase by 1.5 times by 2027, requiring approximately 2,600 new ICT specialists annually, with cybersecurity roles making up 8–10% of this need. This demand for skilled workers in areas like cyber risk management, data protection, and incident response exceeds current and projected graduation rates, resulting in a substantial shortage of trained professionals. To address this gap, Estonia aims to enhance its cybersecurity capabilities through targeted training and multi-role specialists, especially as new regulations and digital expansion increase the need for robust cyber defences across sectors.

In a deeper explanation - OSKA results show us that Estonia's IT related workforce demand is projected to increase by 1.5 times by 2027. Approximately 2,600 new ICT specialists are needed annually. At the same time, only about 7,350 graduates are expected to enter the ICT sector within the next seven years, while the total projected need is over 18,000. Also, the current supply of cybersecurity professionals is far below demand (Kutsekoda, 2022a; 2022b; 2022c). Out of that the need (2600) for cyber security related professions are around 8-10% (meaning 2021 the need was 290 professionals and coming years it will rise to 800, overall calculation was that to meet the demand there is a need for 200 cyber security professionals annually Praxis (2019). This creates a substantial mismatch between the number of trained professionals and the roles that need to be filled in IT and cyber security as well. Given the ageing workforce and low replacement rates (only about 190 professionals can retire annually), this creates a gap that needs to be filled by new workers as it is not sustainable to keep employees who should be retiring.

There is a current and projected future shortage of professionals in roles like cyber security analysts with the skills of GDPR, Big Data and AI. The growing data-driven economy and the expansion of digital services highlight the importance of having robust cyber defences, which further intensifies the demand for cybersecurity specialists. As Estonia has implemented E-ITS, the need to do it is valid to most companies that want to work with any governmental institutions or is one. The need for cybersecurity professionals is expected to rise as Estonia faces stricter regulations, especially concerning cyber security laws. The increasing reliance on digital systems across various sectors is accelerating this demand. Cybersecurity experts will be required to ensure compliance with security requirements in both state and essential service organisations.

There is a marked shortage of professionals with specialised cybersecurity skills. Labour market analyses highlight shortages in the following areas:

- Cyber Risk Management: Professionals who can assess and manage cybersecurity risks are in high demand, particularly in sectors dealing with critical infrastructure and essential services. They currently are also expected to excel at the leadership position, so they should be an expert and leader and supervise themselves at the same time.
- Data Protection and Privacy Experts: The implementation of the EU's General Data Protection Regulation (GDPR) and Estonia's own data protection laws have spurred demand for data protection officers and legal workers with the skills of cyber security, who are currently in short supply.
- Incident Response and Threat Analysis: Many organisations lack skilled personnel capable of managing cybersecurity incidents and analysing cyber threats effectively.

Also, Estonia lacks research professionals that can both do the research, but also to teach. The number of professionals required is not high, but it is an issue that needs to be tackled in the future, sooner rather than later.

At the same time European Cybersecurity Skills Framework Role Profiles lists: Cybersecurity Implementer, CISO, Incidents Responder, Cyber Legal, Policy and Compliance Officer, Cybersecurity Architect, Cyber Threat Intelligence Specialist; Cybersecurity Auditor, Cybersecurity Educator, Cybersecurity researcher, Digital forensic Investigator, Penetration Tester (ENISA, 2022) that we will be using throw-out in this report. This helps us to compare the report results with other Cyberhubs countries, even In Estonia the job market and roles are not always possible to divide in this way. As a small country one needs to take several roles inside its role/position, when working.

To meet future cybersecurity needs, Estonia aims to enhance its national cybersecurity and cyber defence capabilities. The goal is to have a deeper understanding of the evolving cyber threat landscape and effectively address emerging challenges. While specific numbers on the exact number of cybersecurity professionals in Estonia are not mentioned, the importance of cybersecurity and the growing need for professionals in the field are recognized.

2.3.2 Skills

Short: Estonia's cybersecurity workforce faces a skills gap due to rapid technological changes, limited specialized training, and a disconnect between academic preparation and industry needs. Although new technologies like AI and cloud computing are being integrated, professionals often lack the expertise to secure them. High dropout rates in ICT education and bureaucratic barriers to hiring foreign talent further exacerbate the shortage, calling for updated training and collaborative solutions.

In a deeper explanation: the dynamic nature of cyber threats means that cybersecurity professionals need to constantly update their skills. However, many of Estonia's professionals lack continuous training opportunities, leaving a skills gap in the face of rapidly evolving cyber threats. Emerging technologies like artificial intelligence (AI), quantum technologies, blockchain, and cloud computing are being integrated into cybersecurity strategies, but the workforce lacks sufficient knowledge and expertise in securing these technologies.

Also business sector (not IT and cyber security) needs more IT people or hybrid skills engineers that helps them to implement suitable online environments (e.g. remote work solutions that enable joint work) and related services (different options, their advantages and bottlenecks); secure (including personal and data protection principles) communication and collaboration in the digital environment (including online collaborative tools and mobile applications); knowledge of the concepts and principles of data analysis, including the ability to analyse big data; safe use of social media channels and applications.

OSKA highlights the need for a high level of technological understanding, specifically regarding system architectures and security frameworks. This includes knowledge of cyber defence tools, encryption techniques, and security operations. With the growing volume of digital data, professionals must also be skilled in data protection and privacy regulations. This is critical for industries dealing with sensitive information and is becoming more prominent with the enforcement of GDPR and other data protection laws. Leadership in cybersecurity is necessary, particularly for cybersecurity managers and leaders responsible for overseeing the security strategies within organisations. As not every company will have these occupations available, these roles need to be shared with the leadership. For now, the skills of the common leaders about cyber security needs to be updated. This involves preparing companies to plan, develop and execute comprehensive cybersecurity policies.

OSKA report also lists of competencies:

- Cybersecurity professionals need to be proficient in information security protocols, data confidentiality, integrity, and availability. These experts are responsible for ensuring that organisational information systems are protected from unauthorised access and managing the implementation of relevant cybersecurity measures .

- With tightening cybersecurity laws at both the national (Estonian) and EU levels, cybersecurity professionals must be skilled in legal and regulatory compliance. This includes ensuring that organisations adhere to the latest cybersecurity frameworks and security requirements.
- Skills in risk assessment, incident management, and threat analysis are essential. Cybersecurity professionals need to be proficient in identifying and managing risks related to cyber threats and ensuring business continuity by implementing robust defence mechanisms.
- Cybersecurity professionals must possess strong analytical skills to assess security vulnerabilities, design secure networks, and ensure the integrity of an organisation's digital infrastructure.

Praxis report lists cyber security competences: design and development; services and systems maintain; leadership and control; training; prevention and incident management; deterrence and investigation. Report also summaries the mindset of the cyber industry: a. The technical base of cyber security is ensured by a strong IT education and experience acquired in the IT field b. More and more knowledge from fields outside of ICT are being included in the field of cyber security and people with skills c. The specific skills and knowledge of cyber security are learned through additional training and experience. d. In the perspective of the next five years, technological developments will bring new functions for cyber security professionals, which you need to keep up with and accordingly your skills and adapt knowledge (Praxis, 2019).

While Estonia's education system produces graduates in ICT fields, labour market reports indicate that the skills taught often do not align with industry needs, as the industry asks for graduates that have out of school experiences. In their minds:

- Many graduates lack hands-on experience with cybersecurity tools and real-world scenarios. Employers report that new hires often need additional training before they can contribute effectively.
- Most educational programs provide broad ICT knowledge but fail to offer deep specialisations in areas like cybersecurity forensics, cloud security, or advanced threat detection.

Also, many educational institutions in Estonia are struggling to produce enough cybersecurity experts due to insufficient academic staff and outdated curricula that do not address current cybersecurity challenges. The high dropout rate in ICT education programs further exacerbates the mismatch problem, reducing the number of qualified professionals entering the workforce.

There are also several non-formal possibilities to update the skills example participating in training and acquiescing licences that we will discuss more in the chapter of education. The main problem with these is that no-one really evaluates these courses quality. Therefore, on can pay a lot of money and not get the needed skills in the end of the course.

Estonia has also tried to ease the lack of people by attracting foreign talent to meet the growing demand for cybersecurity professionals. However, bureaucratic hurdles and a relatively small domestic market make it difficult to recruit and retain highly skilled international experts.

2.4 Conclusions

Estonia has a well-established national framework for cybersecurity, with strong collaboration between government agencies, military, law enforcement bodies, businesses, and academic institutions. The shift in responsibility from the Ministry of Economic Affairs and Communications to the Ministry of Justice reflects the evolving nature of governance in this area. Estonia’s adoption of a comprehensive national cybersecurity strategy and alignment with EU regulations ensures that the country is well-prepared for current and future cybersecurity threats. In the short term (next 2 years), Estonia will continue to implement its new cybersecurity strategy and enhance coordination between various actors. Medium term (3-5 years), the focus will be on strengthening cooperation between public and private sectors, particularly with the military and international organisations. Long term (beyond 5 years), Estonia will aim to stay a global leader in cybersecurity innovation, research, and industry.

The cybersecurity market in Estonia is growing rapidly, with significant investment from both private and public sectors. Both small and large specialised providers, as well as some bigger IT companies, are growing their business in cybersecurity. The market is projected to grow by over 8% by 2029, emphasising the increasing demand for cybersecurity solutions. In the short term, the market will expand due to stricter cybersecurity regulations and growing digitalization. Medium term, there will be a focus on developing export capabilities and cross-sector collaboration. Long term, Estonia aims to position itself as a global cybersecurity hub, with substantial export opportunities and advanced defence capabilities.

To execute the dream, Estonia is at the same time facing a shortage of cybersecurity professionals, particularly in areas like cyber risk management, incident response, and data protection. The demand for cybersecurity experts is projected to rise by 1.5 times by 2027, with over 200 new professionals needed annually. In the short term, roles like cybersecurity incident responders with skills also to be analysts and data protection officers will be in high demand. Medium term, there will be a growing need for professionals in risk management, incident response, and advanced threat detection. Long term, Estonia will require cybersecurity researchers and leaders to continue driving innovation and defending against emerging threats.

Cybersecurity professionals in Estonia need strong skills in risk management, incident response, and compliance with EU and national cybersecurity regulations. There is a growing emphasis on technological expertise, particularly in cloud security, data protection, and encryption. Soft skills like leadership, analytical thinking, and communication are also crucial. In the short term, Estonia must focus on upskilling current professionals, particularly in compliance, risk management, and threat analysis. Medium term, as technologies like AI and blockchain are integrated into cybersecurity strategies, there will be a need for specialised skills in securing these technologies. Long term, continuous education and innovation will be vital in keeping pace with evolving cyber threats.

Estonia's education system struggles to meet the demand for cybersecurity professionals. Many graduates, with the eyes of the companies, lack the hands-on experience necessary for immediate impact in the workforce, and training programs often fail to provide deep specialisations in areas like advanced threat detection or forensics. In the short term, Estonia needs to focus on filling the skills gap by updating curricula and increasing practical training. Medium term, retraining programs and attracting international talent will be necessary to meet demand. Long term, Estonia's educational institutions must evolve to produce specialists capable of addressing the future landscape of cybersecurity challenges.

3 Questionnaire

3.1 Data collection

The survey was conducted among cybersecurity service providers, as well as private, public, and ICT organisations with a need for in-house cybersecurity professionals in Estonia. The main goal was to assess the most common cybersecurity services, the size of companies involved, and their needs for cybersecurity expertise.

To distribute the survey, we mapped out organisations in Estonia that offer cybersecurity services and/or were looking currently for and/or and or already employing cybersecurity professionals. This resulted in a list of more than 130 organisations that were contacted directly by email and invited to participate in the survey. In addition, Estonian Association of Information Technology and Telecommunications (ITL) distributed the invitation to participate in the survey among its more than 120 members through internal mailing lists, newsletters, social media etc.

A total of 37 respondents participated in the questionnaire, consisting of:

- 16 cybersecurity service providers
- 10 ICT organisations with a need for in-house cybersecurity professionals
- 3 private organisations from other sectors that require in-house cybersecurity professionals
- 3 public organisations needing in-house cybersecurity professionals
- 5 organisations categorised as "other"

This distribution of the company sizes shows that most of the cybersecurity-related companies surveyed are small or micro-sized, with medium-sized companies making up the largest portion of the respondent pool.

This breakdown highlights the involvement of a diverse set of participants across various industries, with cybersecurity service providers being the largest group that answered the questionnaire.

3.2 Results

The survey results highlight the structure of the cybersecurity market in Estonia, where smaller companies dominate the service provider landscape, while medium and large organisations show a greater demand for in-house cybersecurity expertise. Additionally, there is a clear focus on preventive measures, such as training and risk management.

Summary:

- The highest demand roles include Cybersecurity Implementers, Incident Responders, and Penetration Testers. These positions are essential for maintaining robust cyber defences as they directly handle threat analysis, risk management, and incident responses, which are increasingly vital with the rise of complex cyber threats.
- Educational institutions should emphasize skills such as cloud security, data privacy, threat analysis, and secure system design. Additionally, universities must prioritize practical, hands-on experience to ensure graduates are job-ready, aligning more closely with industry needs for skilled professionals who can handle real-world cybersecurity challenges.
- Companies should invest in upskilling ICT staff, reskilling non-ICT employees for general cybersecurity awareness, and offering on-the-job training. Since formal education cannot cover all niche skills, industry certifications and internal training help bridge the gap, ensuring current employees adapt to emerging cyber threats and technologies.
- Most valued skills are Cloud Security, Data Privacy, Threat Analysis, Information Systems & Network Security, Risk Management; Secure Software Development, IT Architecture and Administration Skills, Enterprise Architecture & Infrastructure Design; System Administration & Integration, Analytical Thinking, Communication, Problem-Solving, Adaptability and Willingness to Learn, Legal and Compliance Knowledge.

3.2.1 Overall results

3.2.1.1 Roles and responsibilities

Overall results and figures show the raise of needs from the companies that answered the survey (see figure 1), is that:

- **Cybersecurity Implementer/Expert** current workforce is 114 and there is current need for 85 (current demand is lower than available professionals), 2-Year need is 166 (a significant increase, nearly doubling in demand) and 5+ Year projection is 342 (demand triples over the long term, indicating this role will be in very high demand). Cybersecurity implementers/experts are critical as organizations want to adopt more cybersecurity measures. The long-term demand shows a significant upward trend, highlighting a growing need for professionals with hands-on implementation expertise.
- **Incident Responder** current workforce is 56, needed now 37, 2-Year need is 49 and 5+ Year projection is 85. Incident response is crucial, especially as cyberattacks grow in frequency. Although the current demand is lower than the workforce, the need will increase substantially over the next few years.
- **Penetration Tester** current workforce is 29, needed now 19, 2-Year need is 51, 5+ Year Projection is 99. Penetration testing is one of the fastest-growing areas. This role is critical for identifying vulnerabilities before they can be exploited. The long-term demand will more than triple, making this a highly sought-after position.

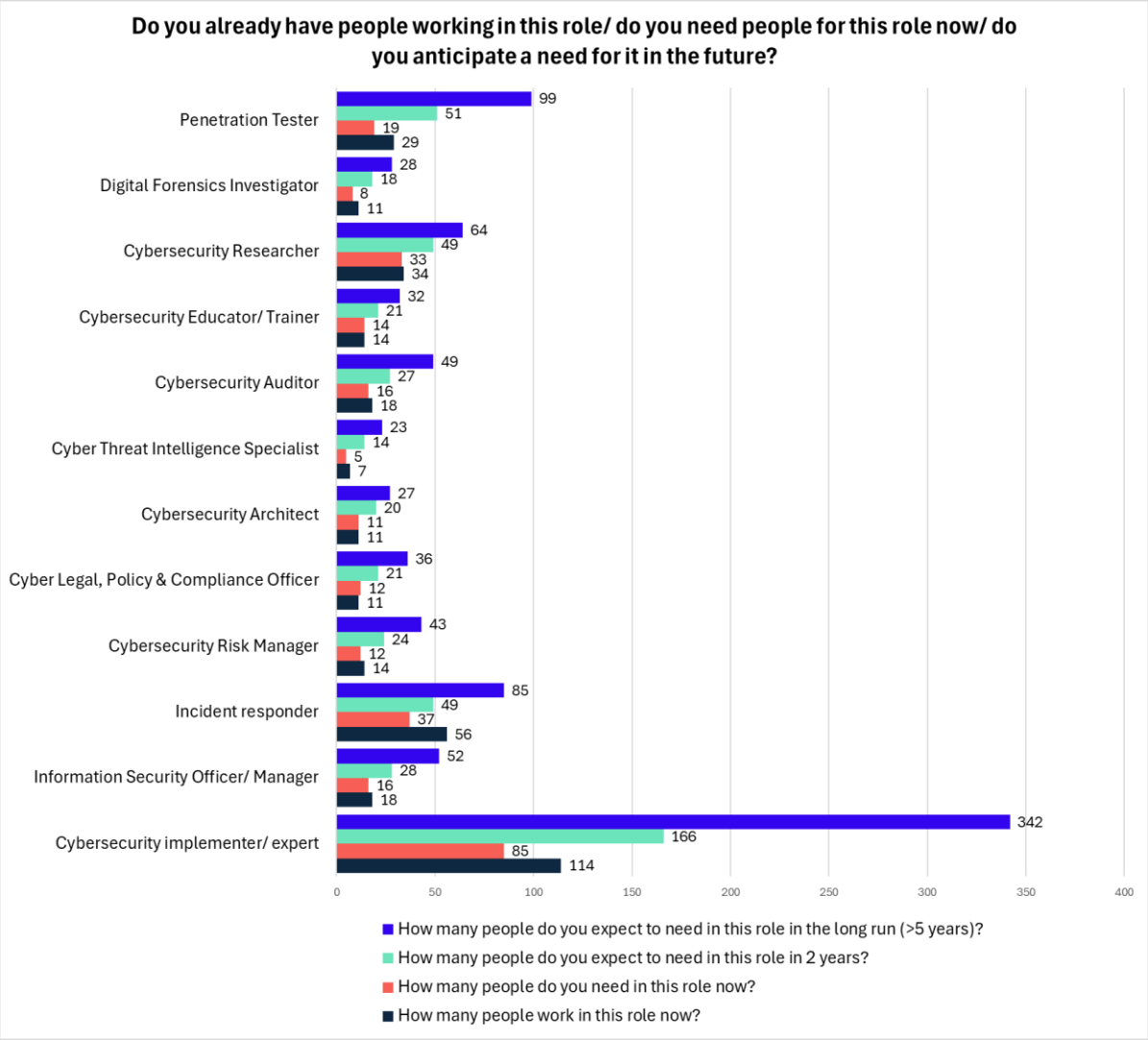

Figure 1: Needs for Roles in the Company

3.2.1.2 Skills analysis

For analysing the skills needed in cybersecurity filed the survey was divided into four parts: cybersecurity skills, IT-skills, organizational skills and transferable skills. The part organizes cybersecurity skills into four main categories - **Cybersecurity Skills**, **IT Skills**, **Organizational Skills** and **Transferable (Soft) Skills**, each highlighting skills that are essential for addressing current and emerging cybersecurity needs.

From the first group (see figure 2) cloud security, threat analysis, data privacy and information systems & network security/cyber resiliency are more valued than others. This does not mean that others are less valuable, this means that employers are needing more help with these and when one references these skills on their survey, they are more easily to get the job. With the growing reliance on cloud services for data storage, software delivery, and overall infrastructure, securing cloud environments is paramount. Breaches in cloud services can lead to massive data loss or exposure. Cloud security is crucial as more companies migrate to cloud platforms like AWS, Azure, and Google Cloud. Threat analysis skill focuses on analysing potential cyber threats to an organization, identifying vulnerabilities, and anticipating attack vectors. It is essential for proactive defence strategies, making it highly important for organizations to mitigate risks before attacks occur. With increased regulations like GDPR and CCPA, ensuring the privacy of user data is not just a compliance issue but also a trust issue. Mishandling sensitive data can lead to severe legal penalties and reputational damage. Data privacy is critical as consumers become more aware of how their data is used. Securing information systems and maintaining the resiliency of networks are foundational to cybersecurity. Organizations need to ensure their networks are secure from breaches and can recover quickly from attacks. This is essential in preventing operational downtime.

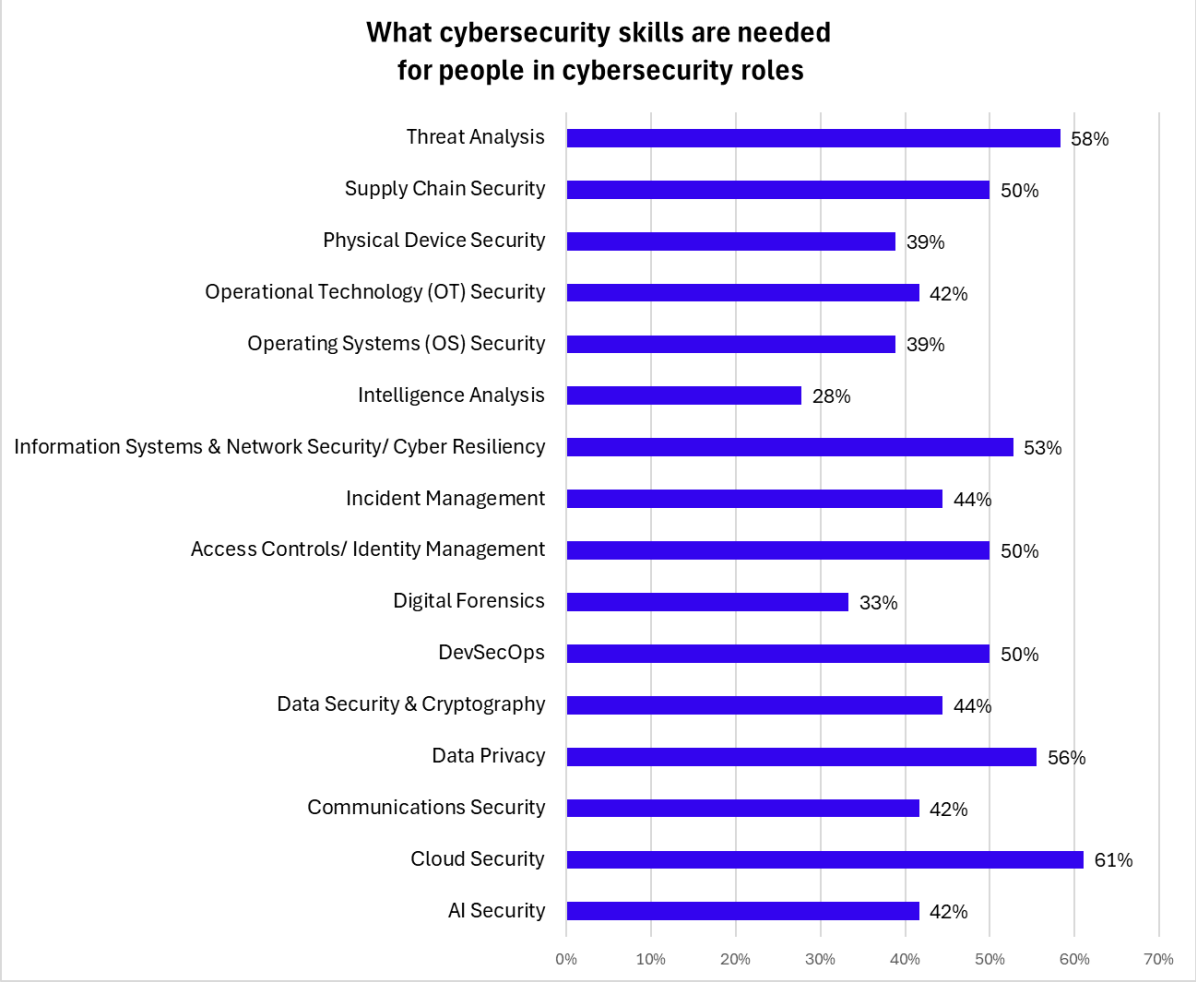

Figure 2: Cybersecurity Skills needed for Cybersecurity Role, % who said "yes" at the survey

From the second group (see figure 3) enterprise architecture & infrastructure design, system administration & integration are more valued than others. These skills are essential for designing the overall IT architecture and ensuring that the infrastructure aligns with the organization's goals and security requirements. With digital transformation, organizations need robust architectures that support scalability, resilience, and security, which explains the high demand for this skill. Administering and integrating various systems is crucial for maintaining a secure and efficient IT environment. As organizations rely on multiple platforms, applications, and services, ensuring seamless integration and administration is key to preventing security loopholes and improving operational efficiency.

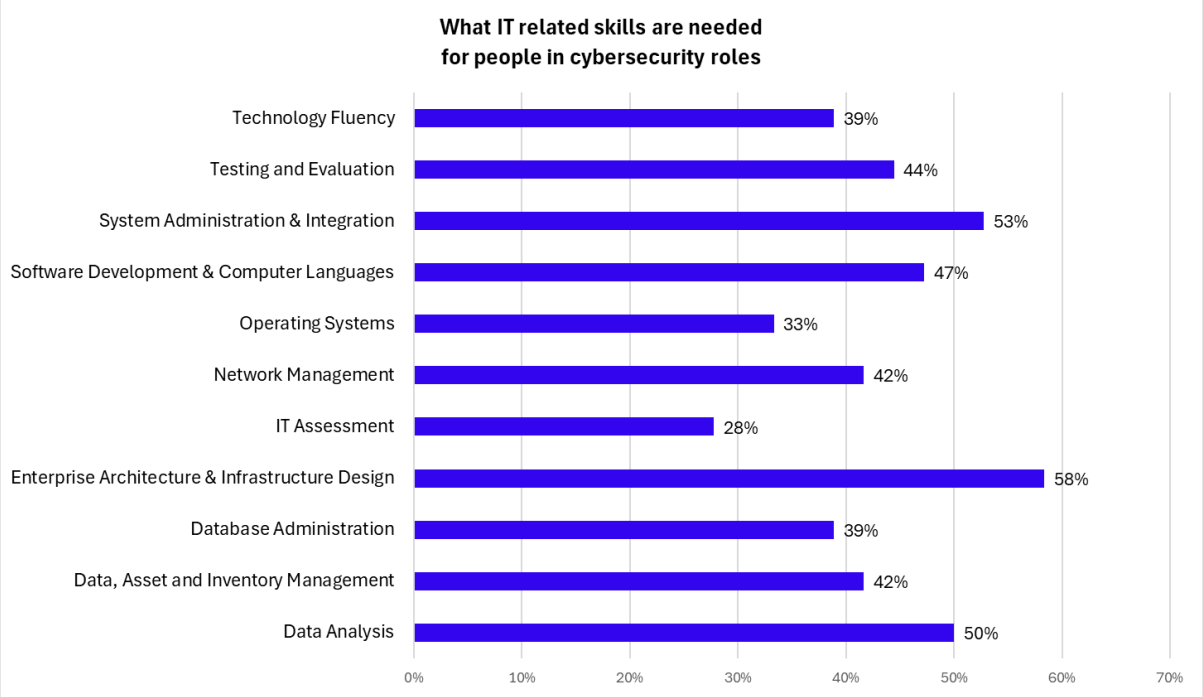

Figure 3: IT-skills needed for Cybersecurity Roles, % who said "yes" at the survey

From the third group (see figure 4) we see that most valued are education and training, delivery & development and risk management. Developing and delivering effective education and training programs is critical, especially in cybersecurity and IT fields where continuous learning is necessary due to evolving technologies and threats. The high demand for this skill reflects the need for upskilling employees and creating a workforce that can respond to new challenges. Managing risks is essential for organizations to anticipate, identify, and mitigate potential threats. In cybersecurity and general business operations, risk management is key to preventing financial loss, reputational damage, and regulatory penalties. This high percentage shows that organizations are heavily prioritizing professionals who can manage and mitigate risks.

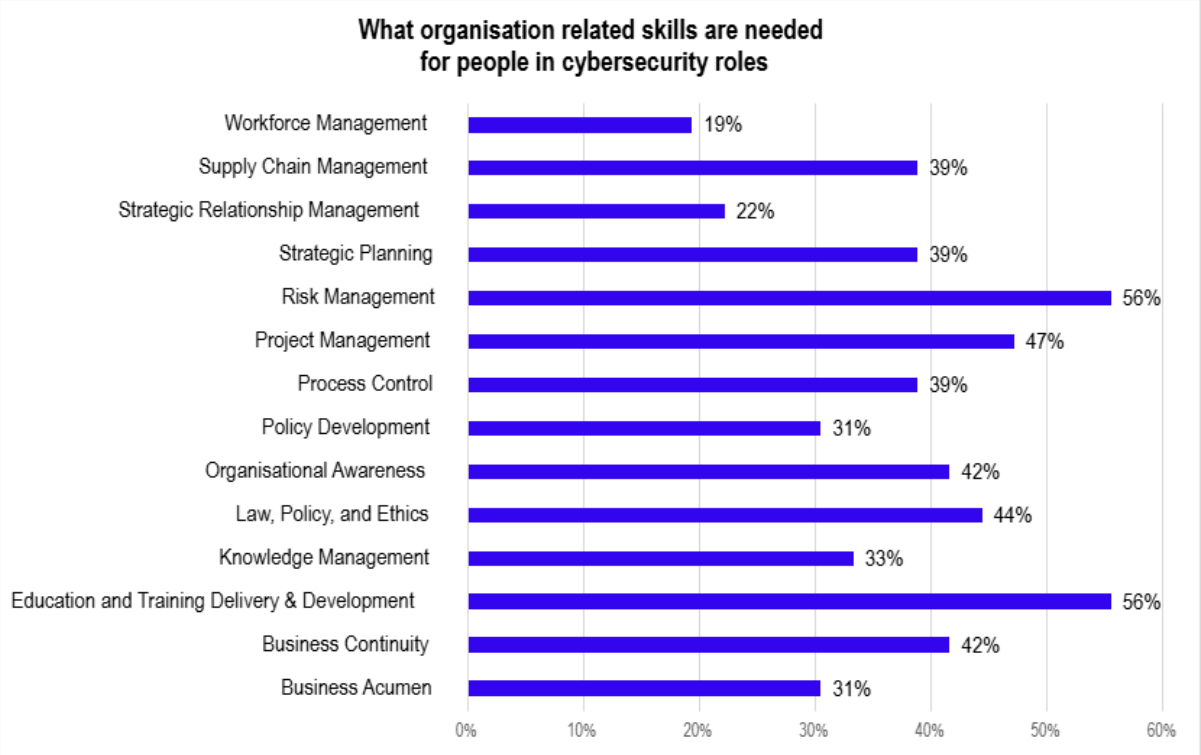

Figure 4: Organizational skills needed for Cybersecurity Roles, % who said "yes" at the survey

From the fourth group (see figure 5) we see that these are the most valued skills for the companies for now. Example **analytical thinking** is one of the most critical soft skills, particularly in technical fields like cybersecurity and IT. Analytical thinking allows individuals to evaluate complex problems, assess risks, and make informed decisions. It is vital for problem-solving and adapting to evolving challenges, making it the top skill in demand. **Communication** is essential across all roles, especially when working in teams or with clients. Effective communication ensures that ideas are clearly expressed, and collaboration is smooth, which is critical for project success and organizational alignment. **Willingness to learn** in rapidly changing fields like technology and cybersecurity is highly valued. Professionals must stay updated with new trends, technologies, and threats, making continuous learning a priority. **Problem solving** - the ability to identify problems, understand their root causes, and develop solutions is crucial. In cybersecurity and technical roles, solving issues quickly and effectively can prevent potential breaches or system failures. Other skills are also not less important as most of them rank 50% or higher on the questioner.

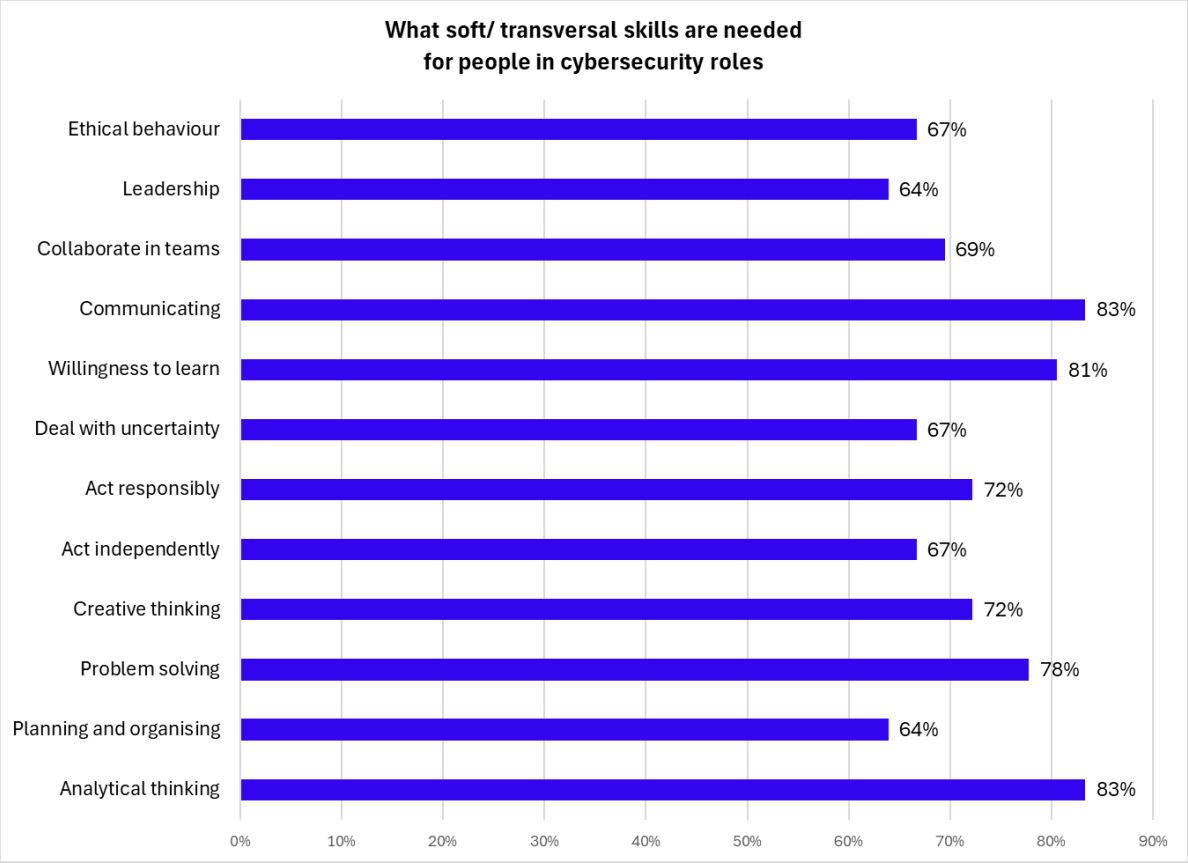

Figure 5: Transferable Skills needed for Cybersecurity Roles, % who said "yes" at the survey

Transferable skills are often considered more important than role-specific or technical skills for several key reasons: Transferable skills like communication, problem-solving, teamwork, and analytical thinking can be applied in various roles, regardless of industry or job function.

Unlike technical skills that may become obsolete due to technological advancements or changes in industry trends, transferable skills remain relevant and useful in any professional environment; the job market is constantly evolving due to technological advancements, economic shifts, and globalization. Transferable skills enable individuals to transition between different job sectors more easily. This is particularly important in today's fast-paced world, where job roles are not static, and careers may span multiple industries. Transferable skills are crucial for long-term career development.

As individuals move up in their careers, technical or role-specific tasks often become less important compared to leadership, communication, decision-making, and strategic thinking. In most workplaces, collaboration and communication are key to success. While technical skills may help an individual perform specific tasks, transferable skills like collaboration, emotional intelligence, and communication allow individuals to work effectively in teams, manage relationships, and resolve conflicts.

- Transferable skills such as problem-solving, critical thinking, and decision-making enable individuals to tackle complex and unforeseen challenges. These skills are highly valued because they allow professionals to approach problems creatively and flexibly, no matter the industry or specific role.
- People with strong transferable skills tend to have higher learning agility, which refers to their ability to learn new information and skills quickly. This adaptability is critical in environments where new technologies or methodologies are constantly emerging, allowing professionals to pick up new technical skills as needed.
- Transferable skills give professionals the flexibility to change careers without starting from scratch. They can leverage skills such as leadership, communication, or analytical thinking to enter a new role or industry, even if they lack specific technical experience.

- Transferable skills not only make professionals more adaptable in their careers, but they also contribute to personal growth. Skills like emotional intelligence, resilience, and time management help individuals lead balanced and successful lives, which in turn enhances their professional capabilities.
- Many transferable skills, such as decision-making, negotiation, and empathy, are critical to effective leadership. As professionals move into leadership roles, they need to inspire, influence, and guide others—tasks that require strong interpersonal and emotional skills.

3.2.1.3 Hiring and upskilling staff

This section discusses the key qualifications and certifications prioritized when hiring cybersecurity professionals. It examines why formal education, certifications, and relevant degrees are highly valued by employers for roles that require foundational knowledge in areas like risk management and regulatory compliance. Additionally, it addresses the industry's openness to hiring skilled candidates without formal education, reflecting findings from previous studies.

Next figure (see figure 6) outlines the importance of various types of educational qualifications and certifications when hiring cybersecurity personnel, along with their respective percentages of importance. Here's an analysis of these factors and why certain qualifications are prioritized more than others when hiring cybersecurity professionals. **Formal professional education relevant for the role** is the most important criterion when hiring cybersecurity personnel. Employers value these because they provide foundational knowledge in areas like security protocols, risk management, encryption, and regulatory compliance. Second important is the certification and thirdly the employers value bachelor/master's degree relevant for the role. At the same time, a smart person is often hired even without formal education credentials. This aligns with the Praxis 2019 report.

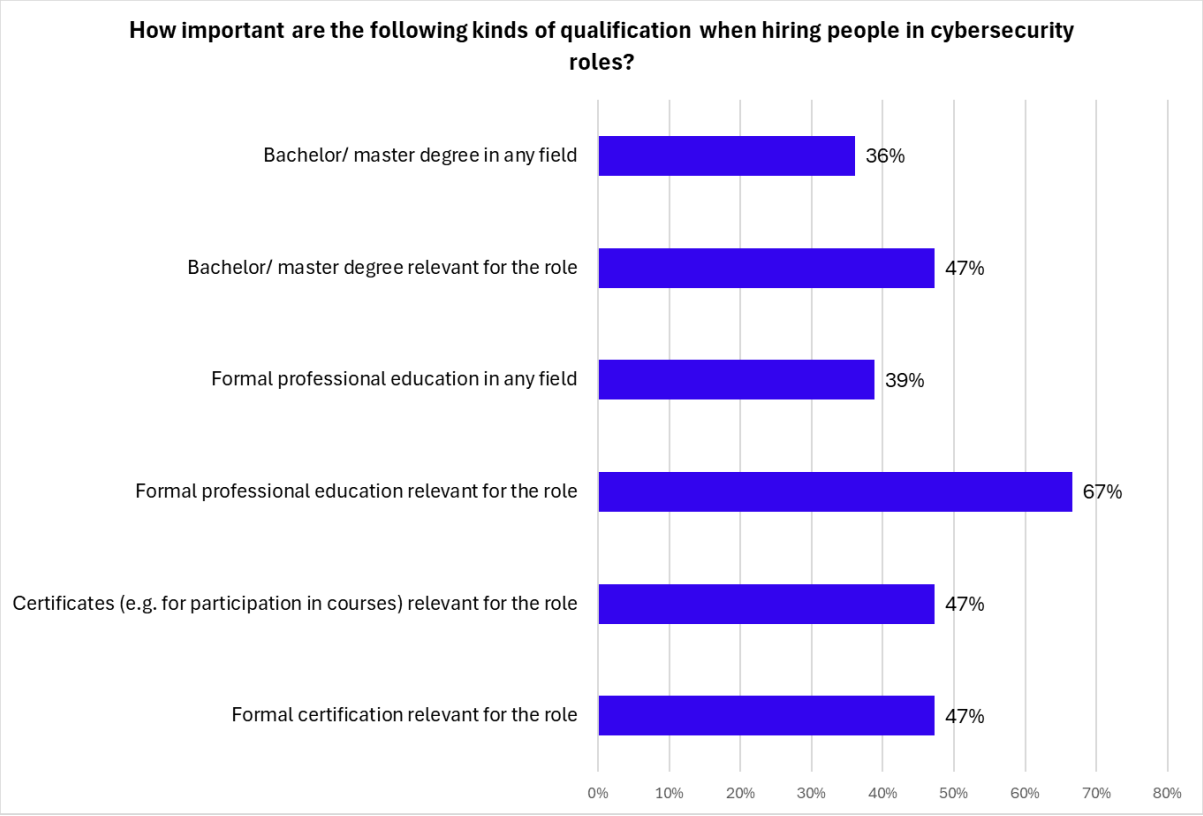

Figure 6: What Is Important when you hire new staff? % who said "yes" at the survey

Next table (see figure 7) presents strategies and approaches that companies are using to build and enhance their workforce in terms of skills and training.

- Upskilling existing ICT personnel is the top priority for most companies. This approach makes sense because these employees already have a foundation in ICT, and further training helps them stay updated with new

technologies, security protocols, and best practices. Upskilling is often more efficient and cost-effective than hiring new talent, as it leverages employees' existing knowledge and familiarity with the company's systems.

- On-the-job coaching and training are a highly prioritized method, showing that companies value practical, hands-on learning. This form of training ensures that employees can apply new skills directly in their work environment, reinforcing learning in real-time.
- Hiring individuals who already possess the necessary skills is a common strategy. While upskilling and reskilling are crucial, sometimes hiring ready-made talent can fill immediate gaps. This is particularly important for roles where specific expertise or experience is urgently needed.
- Training provided by internal staff is also highly valued, reflecting companies' desire to leverage internal expertise and create tailored training programs. In-company training ensures that the learning content is aligned with company-specific needs, culture, and technologies.
- Reskilling non-ICT personnel shows that companies are looking for flexibility and are willing to invest in transitioning existing employees into ICT roles. With the rise of technology in every sector, it makes sense for businesses to tap into their existing talent pool to fill ICT roles.
- Some companies prefer to hire individuals and train them from scratch, especially when there's a shortage of talent with the required skills. This approach allows companies to mold employees into the exact roles they need while also ensuring alignment with company culture.
- External training is often used when the company does not have the internal resources to provide specialized training or when they need to cover industry-standard knowledge or certifications. This can also help bring in a fresh perspective from external trainers.
- Training by external providers, even when conducted internally, is ranked slightly lower. This could suggest that companies prefer to build their training capabilities in-house or seek external training only when there's a very specific skill gap.

Figure 7: How do you hire and upskill your staff? % who said "yes" at the survey

In the next part we will be dividing respondents to two main groups: cybersecurity service providers and companies with the need of in-house cybersecurity professionals. We will not be looking at organisations categorised as other as they are mainly service consumers.

3.2.2 Cybersecurity roles cybersecurity service providers

This part discusses the hiring and upskilling strategies used by companies for cybersecurity roles from companies that provide cybersecurity service to other. It highlights the importance of formal professional education, relevant certifications, and practical training approaches, such as on-the-job training and internal coaching. Upskilling existing ICT personnel is emphasized as a top priority, followed by hiring talent with pre-existing skills when immediate expertise is needed. Companies also value reskilling non-ICT personnel to fill ICT roles and address skill shortages. The section identifies challenges like time constraints, high training costs, and limited external training resources that companies face in enhancing cybersecurity capabilities.

Estonia's cybersecurity industry is expected to expand, particularly in fields like research, penetration testing, risk management, and architecture. The increasingly complex cyber threat landscape will generate a constant increase in demand for expertise from cybersecurity companies as well as in-house teams across multiple sectors.

Among the 16 cybersecurity service providers, the most offered services include:

- Cyber hygiene training (12 providers) – This was the most common service, reflecting an emphasis on raising awareness and improving basic cybersecurity practices.
- Risk management (10 providers) – The second most common service, indicating that organisations focus heavily on assessing and managing cybersecurity risks.
- Security monitoring (9 providers) – Another popular service, showing that real-time surveillance and threat detection is critical for many businesses.
- Testing (8 providers) – Services such as penetration testing, and vulnerability assessments are frequently offered to help organisations evaluate their system defences.
- Crisis management (8 providers) – Providers also play a significant role in assisting companies during and after cybersecurity incidents.
- Other services (10 providers) – Various additional services were offered that did not fit into the main categories.

Discussions also provide insights into the current situation regarding the demand for cybersecurity professionals roles across cybersecurity companies, how much they on average have and need. It also predicts future trends over the next 2 and 5 years, highlighting key roles that will see significant growth in demand.

- In the short term (next 2 years), the rapid growth in demand for cybersecurity companies highlights the evolving threat landscape and the increasing importance of specialised experts. Companies will need skilled managers to oversee security policies, risk assessments, and compliance with regulations. Companies are likely focusing on prevention and proactive strategies rather than response, which could explain the slower growth with some roles.
- Long term (beyond 5 years), companies are prioritising proactive testing of their systems to avoid breaches. Organisations will increasingly focus on hiring professionals to assess, mitigate, and manage cybersecurity risks and who specialise in compliance, policy, and legal aspects of cybersecurity.

Some of the roles at the same times will be acquired by the service provider (example external auditor or legal help). Some higher level and bigger companies also mentioned that they need a cybersecurity architect, to provide overall IT and cyber security service and implement comprehensive security infrastructures. Also, some special companies or institutions will need an example cybersecurity researcher, so uptake the demand due to the rapid development of new cybersecurity threats. These special companies are those that provide cyber security key developments in Estonia, investigate and apply the theoretical and practical security solutions and legal development services for government and universities.

3.2.2.1 Analysis of Cybersecurity Skills, Training Needs, and Hiring Criteria

This section delves into the specific skills that cybersecurity companies and IT departments in Estonia value most, along with insights into training approaches, important soft skills, and challenges related to training personnel in cybersecurity roles.

Cybersecurity-Specific Skills

- Data Privacy (11 companies) and Cloud Security (10) are the most crucial skills for cybersecurity companies. As the world becomes more cloud-centric and privacy regulations (e.g., GDPR) evolve, companies require professionals who can manage secure data storage and cloud infrastructures.
- Information Systems & Network Security/Cyber Resiliency (9) and Threat Analysis (9) are equally vital. These skills help in protecting networks and detecting threats before they lead to incidents, ensuring systems stay operational under cyber-attacks.

IT-Related Skills

- Software Development & Computer Languages (10) ranks highest. This reflects the growing need for cybersecurity professionals who can understand the architecture of the systems they protect and even develop security tools.
- Enterprise Architecture & Infrastructure Design (8) and Risk Management (9) are essential for designing secure systems and managing cyber risks. Professionals with expertise in these areas can create resilient infrastructure and strategies to minimise potential threats.
- Data, Asset, and Inventory Management (8) emphasises the importance of understanding data flow and asset management in preventing unauthorised access and ensuring system integrity.

Other Skills (other)

- Project Management (9) is highly valued, highlighting the need for cybersecurity professionals who can oversee complex security projects and ensure alignment with business goals.
- Policy Development (7) and Law, Policy, and Ethics (7) reflect the importance of legal and regulatory compliance, especially as businesses navigate global security regulations.
- Education and Training Delivery & Development (7) suggests that cybersecurity professionals also need to be capable of training others, which helps build a security-conscious workforce within the organisation.

In addition to technical skills, soft skills are crucial for cybersecurity professionals. The top soft skills identified include:

- Analytical Thinking, Creative Thinking, Willingness to Learn, and Communicating (13 each): These are fundamental for problem-solving and adaptability in the dynamic field of cybersecurity. Analytical and creative thinking allow professionals to find innovative solutions to complex security challenges, while strong communication skills ensure they can articulate their findings and collaborate with other teams effectively.
- Problem Solving and Collaboration (12 each): Cybersecurity issues are often complex and require both individual problem-solving skills and collaboration across departments or teams to ensure an organisation-wide response to threats.

3.2.2.2 Training Approaches and Importance

How to Train?

- Upskilling Own ICT Personnel (15) and On-the-Job Coaching and Training (14): Upskilling is crucial for staying current with new technological developments. On-the-job training helps develop practical, real-time skills, making it the most preferred approach for developing cybersecurity talent.
- In-Company Training by Own Staff (14): Internal training programs ensure that staff can acquire the necessary skills specific to the company's environment and challenges.

Why to Train?

- New (Technological) Developments (14): As cybersecurity evolves rapidly with new technologies, training is essential for keeping up with the latest developments and tools.
- Client Demands (10): External and internal clients often require cybersecurity professionals to possess specific skills that align with their needs.
- New Business Processes (9): When organisations change or adopt new processes, cybersecurity professionals need to adjust their skills to protect new workflows.
- Lack of Initial Skills (7): Many cybersecurity professionals start their jobs without all the necessary skills, indicating that companies value candidates with the potential to learn and grow on the job.

3.2.2.3 Hiring Criteria

One of the most important criteria when hiring cybersecurity professionals is formal professional education relevant to the role. This demonstrates the industry's preference for candidates with structured education, ensuring they possess the foundational knowledge required for cybersecurity roles.

3.2.2.4 Challenges in Training Cybersecurity Personnel

Despite the recognized importance of training, some organisations face backlogs in training personnel for the following reasons:

- Lack of People to Train (2): Some organisations simply lack the staff to provide proper training, which can hinder the growth of cybersecurity expertise within the company.
- Lack of Time (1): Cybersecurity professionals are often so busy managing current threats that they have little time to attend training sessions.
- High Training Costs (1): In some cases, the high costs of training programs make it difficult for organisations to provide adequate learning opportunities for their employees.

3.2.3 Companies with the Need of In-house Cybersecurity Professionals

This section focuses on the skills required for in-house cybersecurity professionals in organisations that are cybersecurity service users, their training needs, and the criteria they consider when hiring professionals.

Cybersecurity-Specific Skills

- Threat Analysis (11): This is the most critical skill for service users, showing a strong focus on the ability to assess and understand emerging threats.
- Cloud Security, Data Security & Cryptography, and Access Controls/Identity Management (10 each): As cloud adoption increases, organisations need professionals to secure their cloud environments. Protecting sensitive data through encryption and managing identities are also crucial to safeguard business systems.
- Supply Chain Security (9): Given the increasing number of supply chain attacks, organisations need professionals who can ensure their partners and suppliers follow strict cybersecurity practices.

IT-Related Skills

- Data Analysis, Enterprise Architecture & Infrastructure Design, Network Management, and System Administration & Integration (9 each): These IT-focused skills are necessary for managing the organisation's infrastructure, networks, and integrated systems. Cybersecurity professionals need to understand both security and IT operations to defend against attacks effectively.

Other Important Skills (other)

- Education and Training Delivery & Development (9): Just like cybersecurity service providers, service users value internal training capabilities, indicating a desire to build a cybersecurity-aware workforce.
- Risk Management (9): Managing and mitigating cyber risks is essential for maintaining business continuity.
- Business Continuity (8): This skill reflects the need to ensure that organisations can continue operating in the face of cyber threats, further emphasising the role of cybersecurity professionals in protecting critical business operations.

In addition the need of soft skills for cybersecurity professionals within organisations highlight:

- Analytical Thinking and Communicating (13 each): These are the top two soft skills, indicating that cybersecurity professionals need strong analytical skills to assess complex situations and the ability to communicate technical information clearly to both technical and non-technical stakeholders.
- Problem Solving and Willingness to Learn (12 each): These skills emphasise the need for adaptability in a rapidly changing field.
- Acting Responsibly (11) and Dealing with Uncertainty (11): Cybersecurity professionals must act ethically and confidently in ambiguous situations, which are common when managing threats and vulnerabilities.

3.2.3.1 Training Approaches and Importance

How to Train?

- Upskilling Own ICT Personnel: Like service providers, organisations focus on upskilling their internal IT teams to handle cybersecurity tasks, ensuring that they are equipped with the latest skills.
- Reskilling Non-ICT Personnel: This reflects a broader effort to educate employees in non-technical roles, emphasising a company-wide approach to cybersecurity awareness and practices.

Why to Train?

- New (Technological) Developments (12): The rapid evolution of technology requires continuous skill development. As new technologies are introduced, organisations need to ensure their staff remains competent.
- Lack of Initial Skills (11): Many professionals start their roles without the required skills, highlighting the importance of on-the-job training.
- Switching Infrastructure (8): When organisations transition to new infrastructure, such as cloud or open-source systems, training is needed to equip professionals with the skills to secure these environments.

3.2.3.2 Challenges in Training

Like service providers, service users face challenges in training personnel for cybersecurity roles:

- Lack of Time for Training (5): Cybersecurity professionals often don't have time to train due to ongoing work demands.
- Organisational Time Constraints (4): Organisations may struggle to allocate time and resources to organise effective training.
- Training Costs (2): Training can be expensive, limiting some organisations' ability to invest in skill development.
- Lack of External Training Options (1): For certain specialised skills, external training may not be readily available.

3.2.4 Comparison: Cybersecurity Service Providers vs. Cybersecurity Service Users and key takeaways

This part compares cybersecurity service providers and companies needing in-house cybersecurity professionals, focusing on key differences in skill requirements, training methods, and hiring preferences. Service providers prioritize data privacy, software development, and privacy management, while in-house roles place more emphasis on data security, cryptography, and network management. Both types value analytical thinking, communication, and problem-

solving as essential soft skills, although service users additionally emphasize reskilling non-ICT employees for broader cybersecurity awareness across the organization.

In a deeper analysis both groups highly value cloud security and threat analysis, showing that these are universal priorities in the field. However, companies that need in-house professionals place more emphasis on data security and cryptography, likely due to the need to protect sensitive information. Both groups value analytical thinking, communication, and problem-solving, which are essential for managing complex cybersecurity issues. A shared emphasis on soft skills highlights the need for cybersecurity professionals to work well in teams and communicate effectively. Both prioritise upskilling their ICT personnel, but companies that need in-house professionals additionally focus on reskilling non-ICT employees to foster a more security-aware organisation. This indicates a more holistic approach to cybersecurity among service users. Time constraints are the most significant barrier for both groups, though service providers are also limited by a lack of trainers. Addressing these time and resource limitations could improve the overall security posture. Both groups highly value formal education for cybersecurity roles. However, companies that need in-house professionals also consider certifications essential, suggesting that they may place more emphasis on validated skills from industry-recognized programs. See the table 2 below.

Aspect	Service Providers	Need of In-house Cybersecurity Professionals	Key Differences
Most Needed Skills	Data Privacy, Cloud Security, Threat Analysis	Threat Analysis, Cloud Security, Cryptography	Service users focus more on identity management and cryptography. Service providers focus more on privacy.
IT-Related Skills	Software Development, Risk Management	Data Analysis, Network Management	Service providers emphasis software development; service users focus more on network and system management.
Soft Skills	Analytical Thinking, Creative Thinking, Communication	Analytical Thinking, Communication, Problem Solving	Both value similar soft skills, but service users prioritise problem-solving.
Training Methods	Upskill ICT personnel, On-the-job training	Upskill ICT personnel, Reskill non-ICT personnel	Service users also prioritise reskilling non-ICT staff.
Challenges in Training	Lack of trainers, Time, Cost	Time, Organisational constraints, Cost	Service providers are limited by the lack of trainers; service users cite organisational time as a barrier.

Hiring Preferences	Formal professional education	Certificates, Formal education	Both value education, but service users also emphasise certifications.

Table 2: Key differences of strategies of cybersecurity Service Providers and Need of In-house Cybersecurity Professionals

3.3 Conclusions

For companies that need in-house professionals, encouraging reskilling programs for non-ICT employees can help create a more comprehensive approach to cybersecurity across the organisation. This could involve in-house training programs that focus on improving general cyber awareness among all employees. Organisations can explore micro-learning sessions or self-paced online training to overcome the challenge of limited time for training. Offering flexible learning options can allow employees to develop their skills without disrupting their regular duties. Both groups should emphasise the value of certifications, which can provide verifiable proof of skills and demonstrate a commitment to continuous learning. To overcome the challenge of limited external training, organisations should collaborate with universities or cybersecurity vendors to develop specialised training programs tailored to their needs.

Cloud Security and Threat Analysis are universally critical skills across both service providers and users. Soft skills like analytical thinking, communication, and problem-solving are equally valued, reflecting their importance in handling complex cybersecurity challenges. Training time and resources are key bottlenecks, but flexible, cost-effective solutions can help address these issues. Both formal education and industry certifications are important when hiring cybersecurity professionals, with a growing need to upskill and reskill employees to keep up with evolving threats.

4 Job vacancy analysis

This part covers **Job Vacancy Analysis**. It explains the data collection process, focusing on major job portals and professional networking platforms in Estonia to assess the demand for cybersecurity roles. The chapter analyses job postings, identifies common keywords, and provides insights into the types of cybersecurity roles in demand across various sectors. Additionally, it highlights gaps in the workforce and sheds light on specific skills and qualifications sought by employers. This information supports understanding how current job market needs align with or diverge from available cybersecurity training and education programs.

The reporting of the job vacancies (185) will be done in collaboration with our provider Abodoo, as well as snapshots from various job portals gathered by hand. There are some analysis of job market and databases (Stat.ee) but they usually do not focus on cyber security market or even IT-market, ta the same time there Is possible to look from the calculator how much one's average salary would be working in this position. So, to do the analysis we could not really use automated solutions (Adodoo had language barriers and) and in the job portals there were only few directly cyber security related job offerings, so we analysed all the portals by hand in July and September-October 2024 and scraped the data to be analysed in this chapter. We also explained the keywords, portals to be used etc.

4.1 Data collection

Estonia has a diverse range of job portals and platforms where companies advertise cybersecurity positions. Here's an overview of the most relevant job boards and online portals for job seekers in the cybersecurity field:

4.1.1.1 Major Job Portals in Estonia

These are the most frequently used general job portals, where companies across sectors, including cybersecurity, regularly post job advertisements.

- **CV Keskus**: One of the largest job portals in Estonia, frequently used for posting cybersecurity and ICT-related jobs. Known for its extensive reach across industries.
- **CV.ee**: Another major job portal widely used by companies in Estonia, offering a range of positions including roles in IT and cybersecurity. It's a go-to platform for both job seekers and employers.
- **Kandideeri.ee**: A popular job board featuring various IT and cybersecurity roles, as well as general job listings across different industries.
- **Otsin Tood**: A site with a growing number of listings, including opportunities for cybersecurity professionals, especially for smaller companies or startups.
- **Töötukassa**: Estonia's official unemployment agency portal, which frequently posts cybersecurity jobs, especially for positions in the public sector or EU-funded projects.
- **Soov.ee**: A classifieds platform where companies can post job listings. It has some IT roles, including a cybersecurity-related position, but not the first place where one can find a job. It's more like a personal ads portal.
- **Okidoki.ee**: A classified ads site where job listings, including IT-related and cybersecurity roles, can be found, but not the first place where one can find a job. It's more like a personal ads portal.

Additionally, jobs are listed usually on the company website or job portals, and then advertised in social media (Facebook) communities where IT and cyber security issues are discussed in public by the experts.

4.1.1.2 Professional and Networking Platforms

These platforms are used for networking and often feature job postings for specialised roles like cybersecurity.

- **LinkedIn**: One of the most significant global professional networking sites, frequently used for advertising cybersecurity roles in Estonia. It is an important platform for both professionals and recruiters in the cybersecurity field.
- **Meet Frank**: A mobile app that connects job seekers and employers anonymously. It is used by tech companies and startups, including those hiring for cybersecurity positions in Estonia.
- **Talendibaas**: A talent platform connecting employers with job seekers, especially in tech sectors. Cybersecurity roles are often posted here, but not available to public to see.

- **GlassDoor:** A online platform that provides insights into workplaces and corporate culture by allowing employees to anonymously review their employers. It offers salary reports, job listings, and interview experiences, helping job seekers make informed decisions about potential employers. Glassdoor is widely used for its database of company reviews, salary information, and interview insights, promoting transparency in the job market and enabling companies to attract talent by sharing their values and workplace environment.

When searching for cybersecurity jobs on portals, both general and specific keywords are used to target listings that relate directly to cybersecurity roles. Below is a breakdown of these keywords and how they help find relevant job opportunities:

Using general and specific keywords allows job seekers to effectively narrow their search for cybersecurity positions. General terms like "cybersecurity", "security", and "risk" help capture a wide variety of roles, while specific terms like "küber", "cryptography", and job titles such as "küberturbe spetsialist" or "Security Risk Management Specialist" help target more specialised positions. Additionally, IT roles with security responsibilities such as "IT-juht", "IT Systems Engineer", and "Linux Cryptography and Security Engineer" are important keywords for finding jobs that may not explicitly list cybersecurity in the title but are crucial for securing IT infrastructure.

4.1.1.3 General Keywords

In Estonian, official terms, job titles, and other terminology often do not have direct English translations, and vice versa, making 1:1 translation between these languages nearly impossible. Additionally, EU keyboards typically lack the characters Õ, Ü, Ä, and Ö, which makes it unlikely that someone in Europe would easily search for Estonian root words online. This limitation adds a level of impracticality to the idea of widespread use or recognition of Estonian terms outside of Estonia.

These broad terms are frequently used across job portals and provide a wide range of results, including roles directly related to cybersecurity or general IT security positions.

- Küber (Cyber): This is a general term that captures various listings related to the cyber domain, including both offensive and defensive roles. In Estonian, *"Küber"* does not exist as a standalone noun; rather, it functions as a prefix or a qualifier, much like an adjective, to denote a connection with cyber-related fields. It is typically used in compound terms such as *"küberjulgeolek"* (cybersecurity) or *"küberruum"* (cyberspace) to specify the cyber aspect of the concept.
- Küberturvalisus (Cybersecurity): A focused term targeting roles specifically dealing with securing networks, data, and systems from cyber threats. It is a core keyword used by job seekers and employers alike.
- Cyber Security/Cyber: These English terms are commonly used in international and local job listings, especially in tech hubs or companies with a global reach.
- Security: Broad but relevant, this keyword helps capture roles that may deal with physical or information security. In cybersecurity job searches, this can include anything from network security to software security. Usually when just used word "security" you will also get list of security guards' positions, that are not related to cyber security.
- Turvalisus (Security): The Estonian term for "security," which can be used to search for both cybersecurity and general security-related roles, including risk management and IT security.
- Cryptography (Krüptograafia): A highly specific keyword that targets listings requiring expertise in encryption technologies, cryptographic protocols, or securing communications. This term is particularly relevant for advanced roles in cybersecurity.
- Risk: This keyword is important for jobs related to cyber risk management, which includes identifying, assessing, and mitigating risks related to cybersecurity threats. Usually when just used word "risk" you will also get list of other positions, that are not related to cyber security, so you need to understand the context.

Specific Cybersecurity Occupation Keywords

These terms reflect specific job titles or roles within cybersecurity and IT security, helping to narrow the search to highly specialised positions.

- Küberturbe ekspert (Cybersecurity Expert): General term for experts in cybersecurity, often senior roles that involve leading security strategies or initiatives.
- Küberturbe analüütik (Cybersecurity Analyst): A specific role involving monitoring, detecting, and responding to security incidents, as well as analysing potential vulnerabilities.
- Küberturbe lahenduste arhitekt (Cybersecurity Solutions Architect): Targets roles focused on designing and implementing secure IT architectures and systems to protect organisations.
- Küberturbe spetsialist (Cybersecurity Specialist): A broad role for professionals who specialize in securing networks, systems, and applications.
- IT Riskihaldur/riskijuht (IT Risk Manager): Focuses on managing cybersecurity risks, assessing potential vulnerabilities, and ensuring compliance with security standards.
- Security Risk Management Specialist: Related to IT risk management, this role emphasises the identification and mitigation of security risks within an organisation.
- Information Systems Security Compliance Engineer: Engineers who ensure that an organisation's information systems meet regulatory, and compliance standards related to security.
- Security Software Engineer: A developer or engineer specialising in building secure software systems and applications.
- Linux Cryptography and Security Engineer: A highly specialised role focusing on cryptographic protocols and securing Linux environments.

IT and Related Occupations

Though not purely cybersecurity-focused, these roles often involve significant security responsibilities. Including these terms in searches can help find security-related jobs that might not be labelled as strictly "cybersecurity."

- IT-juht (IT Manager): While focused on IT management, this role often includes overseeing cybersecurity policies and systems.
- IT võrguadministraator (IT Network Administrator): Network administrators are responsible for securing networks and ensuring their integrity, making this a relevant search term for cybersecurity jobs in networking.
- IT Systems Engineer: System engineers in IT often work on securing large-scale IT infrastructures, making this a broader term that can lead to security-related positions.
- IT-spetsialist (IT Specialist): A general term for IT professionals, often involving security responsibilities, especially in smaller organisations where one person handles multiple IT functions.

Advanced and Research-Oriented Keywords

These keywords target highly specialised or academic roles in cybersecurity, often found in research institutions or universities.

- POSTDOCTORAL RESEARCHER in CRYPTOGRAPHY AND/OR CYBERSECURITY: Postdoctoral roles focusing on advanced research in cryptography or cybersecurity challenges.
- TENURED PROFESSOR OF CYBER SECURITY: Academic positions for teaching and research in cybersecurity.
- POSTDOCTORAL RESEARCHER IN DEVELOPING LARGE LANGUAGE MODELS FOR CYBER SECURITY PROBLEMS: A very specific research-oriented role focusing on applying AI and machine learning to cybersecurity problems.

Keywords for Risk and Data-Oriented Roles

- These keywords focus on IT-related roles that intersect with cybersecurity, particularly in the areas of risk management and data security.
- Finantsriskide kindlustusmaakler (Financial Risk Insurance Broker): Focuses on risk management, potentially relevant for cybersecurity in the context of financial data protection.
- Data Architect: Involves designing secure data systems, making it relevant for searches related to data security.
- Data and AI Engineer: In cybersecurity, data engineers may focus on securing data infrastructure, while AI engineers could work on building systems that detect and mitigate cyber threats.

4.2 Results

Section 4.2 and its subchapters in the document provide a detailed analysis of the **results from job vacancy data** for cybersecurity roles in Estonia. This section examines job listings, focusing on the types of roles in demand and the specific skills and qualifications required by employers. Key insights include an emphasis on cloud security, threat analysis, and data privacy as critical skill areas. Additionally, the section highlights the importance of foundational cybersecurity skills for entry-level positions and specialized expertise in advanced roles, such as incident response and penetration testing. The analysis helps illustrate gaps between available candidates and the skills that are most in demand in the Estonian job market for cybersecurity professionals. In the automated scraping by Abodoo 64 job posts was analysed, while scraping gave us 67+54 additional job posts to analyse, all together 185 offerings were analysed.

4.2.1.1 Analysis of the Scraping-EU Level Dataset

Employers in the EU and World from cybersecurity markets are seeking people from Estonia to join their teams in a wide range of expertise, with an increasing demand for professionals skilled in cloud security, data protection, incident response, and compliance with security frameworks. This scraping-EU level dataset contains various cybersecurity-

related skills mentioned in job descriptions. Here is an overview of the unique cybersecurity skills found in the EU level data:

Common Cybersecurity Skills Required

- Endpoint Protection Platforms (EPP), EDR/XDR – Endpoint detection and response tools.
- Network Security – Implementing and managing secure networks.
- Backup and Disaster Recovery Solutions – Protecting data and systems through backups and recovery methods.
- Data Security & Cryptography – Protecting sensitive data using cryptographic methods.
- Incident Management – Handling and responding to security breaches or incidents.
- Cloud Security – Securing cloud infrastructure and services.
- Operating Systems (OS) Security – Ensuring security on platforms like Windows, Linux, etc.
- Threat Analysis – Analysing and responding to cybersecurity threats.
- Identity Management – Managing user access to systems and services.
- Compliance Standards (SOC 2, HITRUST, ISO 27001, etc.) – Ensuring adherence to various cybersecurity frameworks and standards.
- Security Operations Center (SOC) – Managing security operations and monitoring for threats.
- Penetration Testing (Pentesting) – Testing systems for vulnerabilities through simulated attacks.
- DevSecOps – Integrating security into DevOps processes.
- Digital Forensics – Investigating and analysing cyberattacks and data breaches.
- Vulnerability Assessment – Identifying and mitigating security vulnerabilities in systems.

The dataset highlights a diverse range of cybersecurity skills, with a strong emphasis on cloud security, data protection, and threat analysis. There is a need for compliance with industry standards such as ISO 27001 and frameworks like SOC 2 is a critical aspect, reflecting the increasing regulatory environment surrounding cybersecurity. Incident management and vulnerability assessments are among the most requested skills, indicating a focus on proactive defence and recovery from cyberattacks. Specialised skills like penetration testing, offensive security, and DevSecOps point to a need for deeper expertise in securing complex systems and applications. Skills related to forensics and reverse engineering highlight the need for professionals who can investigate attacks and develop defensive strategies against sophisticated cyber threats.

4.2.1.2 Estonian local scraping by hand Dataset

The demand for cybersecurity professionals in Estonia is varied and robust, with opportunities available across the public, private, and academic sectors. The focus on leadership roles, incident response, and compliance reflects Estonia's ongoing commitment to enhancing its cybersecurity infrastructure. Additionally, the availability of flexible work arrangements in remote or hybrid formats makes these positions more accessible to a global talent pool, helping Estonia maintain its reputation as a cybersecurity hub.

The job listings reflect a wide range of cybersecurity roles, spanning from technical positions like Security Engineers and IT Administrators to leadership roles such as Heads of Security Operations and CISOs (Chief Information Security Officers). This suggests that Estonia has a well-rounded demand for cybersecurity professionals, both at the operational and executive levels. At the same time In summer there were more job listings than in autumn, as currently the IT-Industry is facing temporary cut-offs due to recession and main offerings we looked at are related to engineering and not that much on cyber security filed.

Most Common Roles:

- Cybersecurity Implementer: This category includes roles such as Security Engineers, IT Specialists, and Cloud Administrators. The demand for professionals who can implement and manage cybersecurity measures in organisations is high.
- CISO/Leadership Positions: There is a notable demand for CISOs and other leadership roles, such as Heads of IT Departments and Security Operations Managers, indicating the need for senior-level cybersecurity oversight and strategy in organisations.

- Cybersecurity Researchers: Estonia's focus on innovation and academic research is evident with positions like Postdoctoral Researcher and Technical Researcher at organisations such as TalTech and CCDCOE.
- Cyber Incident Responders: Jobs in security risk management, incident response, and threat intelligence reflect the critical need for professionals to proactively address and mitigate cybersecurity threats.

But there are offerings also to

- Compliance and Legal Focus: Several roles are geared towards legal and compliance aspects of cybersecurity, such as Cyber Legal, Policy and Compliance Officers, and Security and Compliance Managers. This indicates an increasing emphasis on regulatory compliance and information security governance in Estonia.
- Cloud and DevOps Security: Positions like Cloud and Server Services Administrator and Microsoft 365 Administrator show the growing need for cloud security expertise, particularly with more companies migrating to cloud environments.
- Cryptography: Specialised roles like Linux Cryptography and Security Engineer emphasise Estonia's need for experts in cryptographic security, a critical area for secure communications and data protection.

Most positions are based in Tallinn, which serves as a key hub for cybersecurity jobs, though there are options for remote and hybrid roles as well. Companies like Canonical, Bolt, and Pipedrive offer hybrid or remote work, making these roles more flexible and appealing to a broader range of professionals.

Sector Distribution:

- Public Sector: Roles such as Cyber Defense Team Leader and Chief Cyber Certification Specialist are tied to government bodies like the Defence Resources Agency and the Ministry of Economic Affairs and Communications, reflecting Estonia's strong public-sector cybersecurity initiatives.
- Private Sector: There are numerous private companies, including major players like Bolt, Canonical, and Luminor Group, highlighting the demand for cybersecurity professionals across diverse industries (finance, technology, and logistics).
- Academic Sector: Positions like the Postdoctoral Researcher in Developing Large Language Models for Cyber Security Problems at Tallinn University of Technology emphasise the country's investment in cybersecurity research and innovation.

Skills and Education Needed to Apply to the Job

When looking at the scraping results, higher education (bachelor's and master's degrees) in IT, Computer Science, Cybersecurity, or related fields is a common baseline requirement for most roles. Bachelor's degrees are typically the minimum requirement for entry-level and mid-level positions. Master's degrees are often preferred for advanced roles, especially in technical leadership, research, and specialised areas like cybersecurity risk management, information security, and IT systems engineering. Some roles mention applied secondary education in IT, suggesting that practical, hands-on learning and secondary-level degrees can sometimes be sufficient for more operational or entry-level IT roles. This reflects the industry's recognition of skills over formal degrees in certain cases.

For more technical, research, or leadership positions, advanced degrees or PhDs are often preferred. However, relevant certifications (e.g., CISSP, CISM, CEH) are highly valued and can sometimes supplement or replace the need for formal education, particularly in specialised cybersecurity roles. For technical positions, an undergraduate degree in STEM (Science, Technology, Engineering, and Mathematics) is often also accepted. This reflects the flexibility in educational backgrounds for roles that require a strong foundation in technical knowledge, even if it's not specifically focused on IT or cybersecurity.

Degrees in fields like Business, Economics, and Finance are sometimes acceptable, especially for positions related to IT risk management, business continuity, and financial IT systems. This reflects the importance of understanding the intersection of business operations and IT security in certain roles.

Skills Asked from the Offerings

Hard skills from incident response and risk management to compliance, security engineering, and cryptography. The emphasis on a broad experience in cybersecurity technologies, compliance with industry standards, and expertise in both defensive and offensive security techniques highlights the multifaceted nature of cybersecurity roles today. For any cybersecurity professional or team, a combination of these skills is necessary to tackle evolving cyber threats and maintain robust security postures.

- Certifications and trainings such as ISO 27001, NIST Cyber Security Framework, DORA, and OWASP are critical. They demonstrate knowledge of industry standards and ensure that professionals are equipped to handle compliance with regulatory requirements. Security Certifications like CISSP, CISM, and specific certifications around application security are often required to validate one's expertise in cybersecurity. Knowledge of IT compliance frameworks and regulatory standards is important, especially in sectors that handle sensitive data like finance and healthcare. Governance, risk, and compliance (GRC) experience is vital for aligning security practices with business objectives.
- Security engineering - Experience in designing, implementing, and managing security engineering projects is essential, especially with cybersecurity or privacy-preserving technologies. Understanding of zero-trust architectures, which is becoming a key security model, particularly in cloud and network infrastructures. Knowledge of API security and standards like OWASP Top Ten is essential for securing applications and software development. Threat-hunting, forensic analysis, malware analysis, and vulnerability assessments are part of the technical skills required for security operations and incident response. Experience in handling Linux security, cloud security, and web applications (especially securing modern web apps) is crucial for security architects and engineers.
- Strong experience in cybersecurity incident response, including analysing and investigating security alerts and conducting threat intelligence. These skills help mitigate the damage caused by security breaches and improve the speed of recovery. Understanding of malware analysis, forensics, and threat intelligence to respond to complex incidents. Managing Security Operations Centers (SOC), as well as experience with SOC architecture and design, reflects the need to manage complex security environments. Security monitoring using SIEM platforms, threat intelligence tools, and understanding of threat landscapes and attack methodologies (e.g., for Linux and Windows systems) is critical for continuous security monitoring.
- Deep knowledge of risk management principles, including conducting security assessments and prioritising security risks. This involves working with frameworks such as NIST, ISO, and DORA. Vulnerability scanning and risk assessments are key to identifying and mitigating security threats before they can be exploited. Technical understanding of security assessments, such as penetration testing and vulnerability management, ensures that potential weaknesses in systems are identified and remediated.
- Strong understanding of data security principles and the ability to instruct and manage users in case of data security incidents is essential for many roles, particularly in industries dealing with sensitive data like finance and healthcare. Linux cryptography knowledge is important for roles involving cryptographic security. Experience with cryptographic APIs and fundamentals is important for securing communication and data. Roles like cryptography engineers often require these skills to ensure the secure transmission and storage of sensitive information.
- Experience with IT security tools and technologies is essential for identifying potential threats and responding to them effectively. This includes the integration of SIEM tools and managing security vulnerabilities. Knowledge of cloud security is becoming increasingly important as companies move infrastructure to the cloud. Expertise in web application security, including modern threats such as API vulnerabilities and cloud application security. Professionals must be able to validate vulnerabilities and propose solutions for securing applications. Understanding of security best practices for both IT infrastructure and application development is critical for maintaining secure systems.
- Analysing threat intelligence feeds, performing threat-hunting, and conducting risk analyses are core skills for cybersecurity professionals in threat intelligence roles. Understanding of attack and defence methods for systems (Linux, Windows, networks, web applications) ensures that professionals can anticipate and mitigate cyber threats. Knowledge of attack methodologies, defensive techniques, and operational security methods is vital for protecting systems from sophisticated cyber threats.

The broad range of IT (profession-related) skills required in modern IT and cybersecurity roles includes a mix of infrastructure management, programming, automation, security, and risk management expertise. Professionals need to be familiar with cloud environments, scripting languages, secure coding practices, and regulatory compliance frameworks. The growing focus on DevOps, automation, and cloud security reflects industry trends toward more

integrated, scalable, and secure IT environments. Additionally, specialised skills in machine learning, cybersecurity research, and legal aspects of IT show the expanding scope of IT roles across sectors.

The organisational skills listed reflect the need for strong leadership, decision-making, and collaboration abilities across diverse technical and business environments. These skills ensure that leaders can effectively manage teams, plan strategically, and make decisions that align with both business goals and regulatory requirements. Effective project management and client service skills are critical for maintaining high standards of delivery, while risk management and compliance knowledge ensure that businesses remain secure and legally compliant.

The transversal (soft) skills emphasised here are essential across various roles, from technical and managerial positions to client-facing and academic ones. Strong communication abilities, both written and verbal, are paramount, while problem-solving and analytical thinking are critical for overcoming complex challenges. Languages, especially English, are a common thread, enhancing collaboration and communication in multicultural and international settings. Independence, teamwork, and flexibility are crucial traits that enable professionals to thrive in fast-paced, dynamic environments.

4.3 Conclusions

Estonia offers a diverse and extensive range of job portals and professional platforms for advertising cybersecurity roles. Key portals such as CV Keskus, CV.ee, and Kandideeri.ee are widely used for posting cybersecurity-related jobs, catering to various sectors including public, private, and academic institutions. Additionally, networking platforms like LinkedIn and Meet Frank play a crucial role in connecting employers with cybersecurity professionals, especially for specialized roles.

The use of general and specific cybersecurity keywords in job searches helps streamline the process, targeting roles like cybersecurity analysts, IT risk managers, and security software engineers. Estonia's demand for professionals with skills in areas such as cloud security, cryptography, incident response, and compliance continue to grow, with opportunities across different sectors.

The analysis of the EU-level dataset also highlights the increasing need for advanced cybersecurity expertise, focusing on skills such as vulnerability assessment, penetration testing, and cloud security. Estonia's cybersecurity job market is evolving, providing diverse opportunities for professionals ranging from implementers and incident responders to researchers and leadership roles like CISOs. The wide range of roles available demonstrates Estonia's strong commitment to advancing its cybersecurity infrastructure.

5 Desk research (supply)

This part focuses on analysing the availability of cybersecurity education and training options within Estonia. It explores the existing educational programs, courses, and certifications related to cybersecurity and assesses whether these offerings align with the current market demand for cybersecurity skills.

Here we highlight gaps in the alignment between educational programs and the industry's needs, noting that many programs offer broad ICT training without specific focus areas essential for cybersecurity roles, such as advanced threat detection, incident response, and forensics. We also point out that non-formal learning options, like private courses and certifications, exist, but the quality and practical relevance of these are not consistently evaluated. This misalignment and lack of quality assurance can lead to skill gaps in the workforce.

The findings underscore the importance of updating curricula, enhancing practical training elements, and establishing a more structured approach to non-formal education to better meet Estonia's growing cybersecurity needs.

5.1 Data collection

The data collection process for this desk research was conducted using a wide range of sources to analyse the supply of cybersecurity education and training programs in Estonia. The research drew on official reports, labour market studies, company data, and education programs from both public and private institutions. Information was gathered primarily through desk research, including online searches of institutional websites, databases, as well as direct inquiries (via email and phone) to educational institutions.

This dataset includes cybersecurity programs from universities, vocational institutions, and private companies offering certifications. Information gathered Education and Youth board, 2024; Praxis, 2019; Praxis 2023; TalTech, 2022 and Smart Decisions with Haridussilm, 2024.

5.2 Results

International Telecommunication Union (ITU) (2024b) ranks Estonia capacity development 19,74 out of 20. Workforce development in cybersecurity is driven by research, such as OSKA's analysis of cyber competencies, which informs policy recommendations and helps plan educational paths that align with industry needs. This is crucial for ensuring Estonia's workforce meets the growing demand for skilled cybersecurity professionals.

Estonia has developed comprehensive initiatives to integrate cybersecurity education into its state curricula, focusing on enhancing digital competence in youth. Cybersecurity training is embedded within national defence studies across 127 upper secondary schools and 22 vocational institutions. Vocational schools also provide the possibility to participate in a 1-year 5th level program in IT Security Specialist position. For overall education in the lower-level optional national curriculum (under informatic education) and materials are provided in digital hygiene and cyber security for secondary and basic schools from the Ministry of Education and Research, Education and Youth Board. However, challenges remain, including a shortage of skilled teachers and limited course offerings on cybersecurity, despite its importance in national defence.

In higher education, Estonia offers English language holistic programs, such as the bachelor's degree in cyber security engineering from the Tallinn University of Technology (TalTech). This program equips students with practical skills in IT systems security, programming, and ethical norms, preparing them for roles in IT and cybersecurity. The collaboration between TalTech and the University of Tartu also offers a joint MSc in Cybersecurity, which focuses on various specialisations like Cybersecurity, Digital Forensics, and Cryptography. Graduates have excellent opportunities in both technical and managerial roles, benefiting from strong industry connections and practical experiences, including

partnerships with NATO's Cooperative Cyber Defense Centre of Excellence. At the same time the amount who finishes the curriculum is lower than there is a need for young professionals, even though the university dropout rate for the programs is lower than average on other curricula.

To bridge these gaps, Estonia aims to expand cybersecurity courses within general education, fostering early interest in the field. Example from 2023 at the university and starting from 2025 vocational schools for IT filed students, cyber security is a compulsory subject. Extracurricular programs, such as the CyberSpike (KübrNaaskel) competition, help identify talented students for cybersecurity-related military conscription. The educational pyramid in Estonia is strongly gender-skewed, partly due to the unique characteristics of Finno-Ugric male-dominated fields. This creates challenges in attracting girls to IT, requiring specific measures to address this gender imbalance. Consequently, the issues and approaches differ significantly from those in other EU countries, where gender disparity in education may not be as pronounced or influenced by similar cultural factors.

There are several initiatives to provide teachers additional education, but also testing and competitions or summer camps to youth and talents from Tallinn University of Technology, CTF Tech, Information System Authority and others. Also Estonia emphasises public cybersecurity awareness through initiatives like Targalt Internetis (Safer Internet Centre in Estonia), which provides interactive tasks, games, and training for children, parents, and teachers to foster smart internet use and data protection. Collaborative efforts, such as the Women in Cybersecurity - Role Models for Girls project, encourage more female students to pursue careers in cybersecurity, promoting diversity in the field.

Lot of companies' state that they provide cyber security, different levels from cyber hygiene to specialised technical training and certifications. Examples of Tallinn University of Technology, Baltic Computer Systems AS, IT-Koolitus provide official certifications, and Clarified Security, RangeForce, CybExer Technologies, Cyberarch Consulting OÜ provide also gamified training. Others provide different level trainings and consultations, companies like Telia AS, CGI Eesti AS, Cybernetica, CYBERS (Security Software OÜ), Estonian IT Center, OIXIO IT AS, Maecer OÜ, Prevent IT, Securely, KPMG Baltics OÜ, Raulwalter were listed from the questioner above.

Tallinn University of Technology conducts a training program for information security managers within the IT Academy program of the Education and Youth Board, the aim of which is to train more than 200 specialists who could start working as information security managers.

There are also several competitions where cyber security skills are evaluated and trained, for example CyberSpike and Cyber Battle of Nordic-Baltic for the youth 14–25-year-old talents, who later are invited to the EU level European Cyber Security Challenge. As well as NATOs Locked Shield training that brings together military, companies, academics and governmental sectors.

Through a combination of education, extracurricular programs, and public initiatives, Estonia is positioning itself as a leader in cybersecurity capacity-building. The issue remains how to ensure a steady pipeline of skilled professionals and a more cyber-aware society when the need is higher than supply.

5.3 Conclusions

On one hand Estonia has made significant progress in integrating cybersecurity education into national curricula, vocational programs, and higher education, offering diverse pathways for skill development. In the formal level universities offer official cyber security education only in the English language. Vocational schools offer 1-year English language based basic course where the students learn what the cyber security is as a base. Both university BA and vocational school programmes offer basic level of understanding of everything. Other IT programmes offer 1-2 course of secure programming or secure administration skills. Masters level The Cyber Defense program focuses to give a comprehensive foundation in cybersecurity, with opportunities for in-depth study in cyber defense, digital forensics, or

cryptography, depending on the chosen specialization. Graduates are prepared for roles as technical cybersecurity specialists, incident management experts, or analysts, and are well-positioned to pursue doctoral studies.

However, challenges remain, particularly in the shortage of skilled educators, the limited number of specialized cybersecurity courses, and the overall supply of professionals not meeting the growing demand. So, in another hand when discussing the relationship between academia and practice, it should be stated plainly that universities in smaller countries often face survival challenges. Previous solutions, such as relying on international students, are now only partially effective due to the deteriorating security situation and the impacts of COVID-19. Consequently, there may be limited time, funding, or resources left to address issues beyond mere survival. Also, there is an issue to prevent private companies from capturing young audiences with flashy branded products. In other words, how can universities ensure that diversity (like Linux) continues to be taught, so students don't get the impression that only Apple and Microsoft exist?

Also, we need to point out that Estonian is not an Indo-European language, which makes the creation and management of professional terminology a unique challenge. It can be said that the Estonian translations of GDPR and NIS 2 contain so many errors that professionals often avoid using them. This language barrier and terminological difficulties make conducting training significantly more challenging. Since cybersecurity is taught and research is published primarily in English, Estonian terminology in this field cannot develop at the same pace, which poses a significant problem. This creates an additional burden for the industry, which ideally should not be responsible for developing Estonian-language terminology. Achieving a balance between technicians and lawyers remains an ideal that has yet to be realized. As a result, legal language often disregards ISO standards and established terminology, leading lawyers to create impractical virtual constructs (such as the so-called "cloud regulation") that do not function effectively in real-world applications.

While Estonia has many private sector programs offering certifications and practical training, the need to expand formal education pathways and engage younger students through extracurricular activities is essential to closing the skills gap. Collaborative efforts between the government, educational institutions, and private companies will be critical in ensuring a steady flow of skilled cybersecurity professionals to meet future demand.

6 Expert panel

This part presents insights from an expert panel aimed at identifying current and future needs in Estonia's cybersecurity workforce. It covers discussions on essential cybersecurity roles, skills requirements, and training needs for professionals in the industry.

Key takeaways include:

- The panel emphasized immediate needs for roles like penetration testers, incident responders, and cybersecurity implementers. In the coming years, there will be growing demand for cybersecurity architects, compliance officers, and cyber threat intelligence officers.
- Experts stressed the need for both technical and soft skills. Critical technical skills include threat analysis, secure system design, and data protection, while valued soft skills are analytical thinking and communication. Training programs are encouraged to focus on practical, hands-on experience to align with industry expectations.
- The panel recommended enhancing collaboration between the public and private sectors to address skills gaps and advocated for reskilling existing employees to meet cybersecurity needs. The expert panel's feedback aligns with the document's broader emphasis on the importance of structured, adaptable education pathways and continuous upskilling to keep pace with evolving cybersecurity challenges.

6.1 Data collection

The expert panel discussions served as a qualitative approach to capture the evolving needs and challenges of Estonia's cybersecurity workforce. The expert panels took place in two sessions on 3.06.24 and 10.06.24 and each lasted for 2 hours. The panel was conducted in real life. There were 13 participants in total: experts from 6 CS related companies or organisations (of different sizes, i.e. from micro to large), 7 ICT or private/public organisations that need in-house cybersecurity professionals (including one education provider).

Questions that were discussed: What will the demand for cybersecurity roles be in the next two years and in the long run? What skills will be important in those roles in the next two years and in the long run? How should training/ education providers adapt to overcome or prevent skills mismatches in the next two years and in the long run?

Additional materials used to conduct the panel discussion was European Cybersecurity Skills Framework Role Profiles and skills (technical, nontechnical).

6.2 Results

During the discussions, multiple key topics were raised and validated by the group, providing insight into the short- and long-term needs in cybersecurity roles, skills, and training.

6.2.1 Cybersecurity roles

The cybersecurity landscape is rapidly evolving, driven by increasing digitalization, the rise of new technologies (especially using cloud solutions, changes in crypto), and the growing complexity of cyber threats (example implementing Estonian cybersecurity standard). Organisations of all sizes are recognizing the critical importance of robust cybersecurity measures, but currently, the cybersecurity workforce is strained, with a noticeable shortage of professionals who possess the necessary technical and non-technical skills to meet the demands of the industry. This is particularly evident in small to medium-sized enterprises (SMEs) in Estonia, where a single individual often must cover multiple roles due to resource constraints. In contrast, larger organisations can afford to have specialised positions, but they still struggle to find qualified candidates to fill these roles.

The most needed in the next two years are: penetration testers, CISO, cybersecurity Implementer, cyber incident responder, cybersecurity auditors. In five years, the need for cybersecurity architect, legal policy and compliance officer and cyber threat intelligence officer may also emerge, but we would not necessarily see it reflected on the job market, as professionals inside the companies would be developed for the positions or would receive these roles as additional responsibilities, while keeping their current position in the company.

In the immediate future, the demand for certain cybersecurity roles is expected to be particularly high:

- Penetration Testers (Pentesters): There is an urgent need for pentesters who can identify and exploit vulnerabilities in systems before attackers do. Despite the rise of automation, which may eventually handle simpler tasks, pentesters remain crucial for complex and nuanced security assessments.
- Chief Information Security Officers (CISOs): The role of the CISO is becoming increasingly important as organisations seek to integrate cybersecurity into their overall business strategy. CISOs must not only have a deep understanding of technical security issues but also be able to communicate effectively with other executives and stakeholders. Currently, many CISOs are also taking on responsibilities that overlap with those of incident responders and IT specialists, highlighting a gap in specialised roles.
- Cybersecurity Implementers: These professionals are needed to apply and integrate security solutions across various platforms and environments. Implementer role is particularly critical in small companies, where they may also need to handle broader IT responsibilities.
- Cyber Incident Responders: As the frequency and complexity of cyber incidents increase, the demand for skilled incident responders is rising. These individuals must be able to analyse logs, investigate security breaches, and ensure that data integrity is maintained, especially when dealing with legal and regulatory frameworks.
- Cybersecurity Auditors: With the introduction of more regulations and standards, such as the Estonian Information Security Standard, the need for auditors who can ensure compliance is growing. These professionals must be well-versed in both local and international standards.
- Looking ahead to the next five years and beyond, the demand for certain cybersecurity roles is expected to evolve:
- Cybersecurity Architects: The need for professionals who can design and oversee the implementation of comprehensive cybersecurity frameworks will increase. These architects must understand the broader IT landscape and how cybersecurity fits into it. Developing a cybersecurity architect typically takes around 10 years of experience, which poses a challenge for organisations that need these skills immediately.
- Legal Policy and Compliance Officers: As regulations continue to multiply and evolve, the demand for professionals who can navigate the complex legal landscape of cybersecurity will grow. These roles will be essential in ensuring that organisations remain compliant with both local and international laws. These roles are usually provided as services from other providers or are under the role of CISO
- Cyber Threat Intelligence Officers: While the need for threat intelligence is clear, the high cost of hiring dedicated officers means that in many organisations, this role is distributed among other cybersecurity staff, particularly in Security Operations Centers (SOCs). However, as cyber threats become more sophisticated, the demand for specialised threat intelligence will likely increase.
- Cybersecurity Researchers: Although few organisations currently require dedicated researchers, their role in advancing cybersecurity knowledge and developing new strategies will become more important over time for some companies (example 2-3 organisations will want to hire 30-40 people to keep up with the demand in Estonia and EU). Researchers may also transition into other roles, such as cybersecurity architects, as they gain experience and expertise.

6.2.2 Skills for cybersecurity professionals

Over the next two years and beyond, cybersecurity roles will require a blend of technical and non-technical skills. As the field evolves, professionals will need to continuously update their skill sets, particularly in areas like AI security, cloud security, and secure coding. At the same time, non-technical skills such as strategic planning, communication, and ethical responsibility will become increasingly important, especially for leadership roles. Training and education programs must adapt to these emerging needs to ensure that the cybersecurity workforce is prepared for future challenges.

IT and cyber skills that are important to cybersecurity investigative roles and could be learnt by formal education are: system administration and Integration, network management, data privacy, information system and network security,

cyber resiliency. Some experts also mention AI security, depending on the role it should be provided in MA or PD level. These roles also need nontechnical skills like problem solving, analytical thinking, supply chain management, strategic planning, collaboration in teams, risk management, business continuity, law, policy and ethics. Half of the skills should be provided in vocational or BA level. Depending on the roles some new skills emerge like cyber sec responder roles formal education example will include access controls and identity management, some even include data security and cryptography, intelligence analysis and threat analysis, risk management, organisational awareness, policy development, process control to master's level. Some argue that while law policy and ethics for them they should learn it themselves (non-formal education).

At the same time nonformal education could give hand with skills like testing and evaluation, incident management and technology fluency, but also communication, act independently and deal with uncertainty. Some experts also mentioned DevSecOps, Cloud Security as part of non-formal education that they expect specialists to learn by themselves. From personal development the expectation is that act responsibly, ethical behaviour, willingness to learn comes from the person itself.

Technical Skills:

- System Administration and Integration: Essential for maintaining and securing IT environments. Professionals need to understand how to integrate various systems securely, ensuring that they work together without introducing vulnerabilities.
- Network Management: Critical for protecting an organisation's network infrastructure. This includes managing firewalls, intrusion detection systems, and ensuring secure communication across the network.
- Data Privacy and Information Security: As regulations like GDPR and other data protection laws become more prevalent, professionals must have a deep understanding of data privacy principles and how to implement them within organisations.
- AI Security: With the increasing use of AI in cybersecurity, understanding how to secure AI systems and defend against AI-driven attacks will become increasingly important.
- Cryptography: As cryptographic standards evolve, especially with the advent of post-quantum cryptography, professionals will need to stay updated on the latest techniques to secure communications and data.
- Secure Coding: As AI and automation take over more routine tasks, secure coding practices will be crucial for developers to ensure that their code is free from vulnerabilities. This skill needs to be integrated into developer training from the outset.
- Incident Management: The ability to quickly and effectively respond to security incidents is vital. This includes analysing logs, containing threats, and ensuring that systems are restored securely.
- Technology Fluency: As technology evolves, cybersecurity professionals need to stay fluent in new tools and platforms, ensuring they can effectively protect and manage new types of systems and technologies.

Non-Technical Skills:

- Problem Solving and Analytical Thinking: Cybersecurity professionals must be able to think critically and analytically to identify and mitigate threats. This includes understanding complex systems and how they can be exploited.
- Strategic Planning: For roles like CISOs and Cybersecurity Architects, the ability to plan and implement long-term security strategies is crucial. This involves understanding the broader business context and aligning security efforts with organisational goals.
- Collaboration and Communication: As cybersecurity increasingly requires coordination across different departments, professionals must be able to communicate effectively with both technical and non-technical stakeholders. This is particularly important for CISOs and other leadership roles.
- Risk Management: Understanding and managing risks is central to cybersecurity. This includes identifying potential threats, assessing their impact, and implementing measures to mitigate them.
- Law, Policy, and Ethics: As legal and regulatory frameworks become more complex, cybersecurity professionals must be knowledgeable about relevant laws and ethical standards. This is especially important for roles involving compliance, such as Cyber Legal Officers and CISOs.
- Supply Chain Management: As cybersecurity threats increasingly target supply chains, understanding how to manage and secure supply chains will become an essential skill.

- Business Continuity Planning: Ensuring that organisations can continue to operate during and after a cyber incident is a critical skill. This involves planning for contingencies and ensuring that recovery plans are in place.

Emerging Skills:

- AI and Machine Learning: As AI becomes more integrated into cybersecurity, professionals will need to understand how to secure AI systems and use AI tools effectively to enhance security measures.
- DevSecOps: With the shift towards integrating security into the development process, understanding DevSecOps practices will be crucial. This includes automating security checks within the software development lifecycle.
- Cloud Security: As more organisations move to the cloud, securing cloud environments will be an essential skill. This involves understanding cloud architectures and how to implement security controls specific to cloud services.
- Digital Forensics: Although specialised, digital forensics will remain an important skill for investigating cyber incidents and providing evidence in legal contexts.
- Ethical Behaviour and Responsibility: While often seen as a personal trait, ethical behaviour is increasingly important in cybersecurity. Professionals must be trusted to handle sensitive information and make decisions that protect the organisation and its stakeholders.

6.2.3 Training of cybersecurity professionals

To overcome and prevent skills mismatches in cybersecurity, training and education providers must be proactive in adapting their programs to the evolving needs of the industry. This involves integrating practical experience, focusing on emerging technologies, enhancing soft skills, offering flexible learning opportunities, and maintaining a strong connection with industry. By doing so, they can ensure that graduates are well-equipped to meet the demands of both current and future cybersecurity roles.

The panellists conveyed the idea that formal education is nice to have or basic, but when hiring they would be more interested in personal experiences and job experiences as they would be hiring more advanced personnel. When hiring straight from the school they are still interested in real-life experiences from practice or additional or volunteer work (technical and nontechnical) experiences that would be harder to prove. While “act responsibly” is important to acquire, the feeling was that it should be a personal trait, at the same time no-one really has seen that one is not responsible in real life or at least it will not pop out in the interview. Only youngsters that apply when they do not even come to the interview, then you can state that they may not be acting in a responsible way.

Emphasise Practical Experience and Hands-On Learning:

- Educational programs should incorporate more practical, hands-on experiences. This could include lab exercises, simulations, and real-world projects that allow students to apply theoretical knowledge in realistic scenarios. For example, developing secure coding practices through practical coding exercises or using AI tools in simulated security environments.
- Strengthen partnerships with industry to provide students with internships and apprenticeships. These opportunities allow students to gain real-world experience and understand the daily challenges of cybersecurity roles. This is especially crucial in roles like incident response and penetration testing, where practical experience is invaluable.
- Institutions should collaborate closely with cybersecurity companies to ensure that their curricula align with current industry needs. This could involve regular consultations with industry experts, updating course content based on the latest technologies and threats, and offering specialised certifications that are recognized by employers.

Focus on Emerging Technologies and Skills:

- Given the increasing role of AI in cybersecurity, training programs should incorporate AI and machine learning courses. This will prepare students to secure AI systems and leverage AI for security purposes. Additionally,

offering advanced modules on AI security at the master's level can help bridge the gap for professionals transitioning into these roles.
- As DevSecOps practices and cloud computing become more prevalent, educational programs should offer dedicated courses on these topics. Students should learn how to integrate security into the development process and how to secure cloud environments, reflecting the shift towards these technologies in the industry.
- With the advent of post-quantum cryptography, programs should ensure that students are up-to-date with the latest cryptographic standards and techniques. This will be particularly important as the industry prepares for new types of encryption and security protocols.

Enhance Soft Skills and Cross-Disciplinary Training:

- Cybersecurity professionals must be able to communicate effectively with both technical and non-technical stakeholders. Training providers should include courses on communication, teamwork, and leadership, particularly for roles like CISOs and cybersecurity architects. Role-playing exercises, group projects, and presentations can help develop these skills.
- Ethics training should be integrated into all cybersecurity programs. As professionals will be handling sensitive data and making critical security decisions, understanding ethical implications and acting responsibly is essential. Case studies and discussions on real-world ethical dilemmas in cybersecurity can help instil these values.
- To prepare students for leadership roles, educational programs should include training on business continuity, risk management, and strategic planning. This will ensure that future CISOs and cybersecurity architects can align security strategies with overall business goals.

Flexible and Continuous Learning Opportunities:

- Offer modular courses and stackable credentials that allow students to build skills progressively. This approach enables learners to update their knowledge as new technologies and threats emerge, making it easier for professionals to stay current without committing to full degree programs.
- Combine online learning with in-person workshops and labs to provide flexibility while ensuring that students receive hands-on experience. Online modules can cover theoretical aspects, while in-person sessions can focus on applying those concepts in practical settings.
- Encourage a culture of lifelong learning by offering continuing education courses for professionals already in the field. This could include short courses, workshops, and certifications on emerging topics like AI security, cloud security, and advanced cryptography.

Address the Gap Between Academia and Industry:

- Regularly update curricula to reflect the latest industry standards, technologies, and threats. This can be achieved through ongoing collaboration with cybersecurity practitioners and organisations, ensuring that academic programs remain relevant and aligned with the needs of employers.
- Use case studies, real-world problem-solving exercises, and simulations that reflect the current cybersecurity landscape. This approach helps students understand the practical implications of their learning and prepares them to handle the complexities they will face in their careers.
- Involve cybersecurity professionals in teaching roles, either as adjunct professors or guest lecturers. This not only bridges the gap between theory and practice but also provides students with insights into current industry practices and challenges.

Addressing Specialized Needs in Smaller Markets:

- In smaller markets like Estonia, where companies often need generalists rather than specialists, training programs should offer multi-disciplinary courses that cover a broad range of cybersecurity skills. This allows graduates to adapt to various roles within an organisation.
- Offer customised learning paths that cater to the specific needs of smaller companies. For example, a single course could combine elements of incident response, system administration, and network security, providing a comprehensive skill set for students who will work in environments where they need to cover multiple roles.

6.3 Conclusions

In small to medium-sized enterprises (SMEs) in Estonia a single IT-professional often must fill multiple cybersecurity (and IT) roles due to resource constraints. Therefore, these companies look to hire professionals with a very broad skillset and good amount of previous experience. In contrast, larger organisations can afford to have specialised positions. Nevertheless, they still struggle to find qualified candidates to fill these roles.

There are several cybersecurity roles that are especially in demand in the short run, such as: penetration testers, CISO, cybersecurity Implementer, cyber incident responder, cybersecurity auditors. In the next five years, it is foreseen by the expert panels that the demand will grow to fulfil the roles of cybersecurity architect, legal policy and compliance officer and cyber threat intelligence officer. On the one hand, panellists claim that they do not require a degree to hire cybersecurity professionals. On the other hand, they look for a strong technical foundation and vast experience, as well as are quite critical of the level of skills (acquired from university etc.) of new professionals trying to enter the job market.

The academia highlights that it is increasingly hard for students to find internships and graduates to find entry-level jobs. Hiring companies cite an overload of work, due to which there are not enough resources to supervise and teach, which is why positions are mostly opened for experienced professionals. Expert panel feels that academia and industry have been drifting apart for a while, which results in a mismatch in actual skills/knowledge needed on the market and what is taught today.

7 Conclusions

Estonia has made significant strides in developing a comprehensive cybersecurity framework, driven by its digital leadership in Europe and recognition on the global stage. The increasing complexity and frequency of cyber threats, such as Distributed Denial-of-Service (DDoS) attacks and ransomware, continue to challenge Estonia's critical infrastructure, underscoring the importance of robust cybersecurity measures.

The demand for cybersecurity professionals in Estonia is rising rapidly, yet there is a stark mismatch between the skills required and the workforce available. The existing educational systems are producing fewer specialists than needed, and while Estonia's emphasis on digital education is a strength, it has not yet managed to fully close the gap between market demands and available talent.

Small to medium-sized enterprises (SMEs) are particularly affected by this shortage, often requiring IT professionals who can perform multiple roles due to limited resources. Larger companies, while more able to hire specialised professionals, also struggle to find talent with the necessary expertise. Roles such as penetration testers, cybersecurity implementers, and incident responders are in high demand and expected to grow significantly in the coming years.

To address this gap, Estonia is taking steps to enhance cybersecurity education and training programs, focusing on real-world applications and industry-relevant skills. National initiatives, such as upskilling current professionals and fostering international talent, aim to meet the growing demand for cybersecurity expertise. However, Estonia must overcome challenges related to aligning academic curricula with industry needs and ensuring that its education system can keep pace with rapid technological advancements.

Looking forward, continuous investment in education, research, and innovation will be critical for Estonia to maintain its position as a global leader in cybersecurity. A collaborative approach, involving government, academia, and industry, is essential to develop a workforce capable of defending against the increasingly sophisticated cyber threats of the future.

7.1 Cybersecurity roles

The cybersecurity roles in Estonia reflect the country's rapid digitalization and the increasing complexity of cyber threats. Across various studies, expert panel discussions, and questionnaire feedback, a few key roles have emerged as essential for Estonia's future cybersecurity landscape.

Roles needed:

- Current High-Demand Roles: Secure Software Developers are the most needed role according to the job market, but also people with skills of Penetration Testers are needed implementers and responders as well. Testers and implementers are one of the most urgently needed roles due to the growing necessity of identifying vulnerabilities before they are exploited. This role is particularly vital for both SMEs and larger organizations; Chief Information Security Officers (CISOs): As organizations prioritize cybersecurity within their business strategies, the demand for CISOs continues to rise. They are expected to have a blend of technical expertise and leadership skills; Cybersecurity Implementers: Implementing security solutions is essential, especially for smaller companies where professionals may need to cover broader IT responsibilities; Cyber Incident Responders: The frequency and complexity of cyberattacks have led to a critical need for professionals who can handle incident detection, response, and resolution; Cybersecurity Auditors: With increasing regulatory frameworks, auditors are necessary to ensure compliance with both local and international standards.
- Evolving Future Roles: Cybersecurity Architects: As systems become more integrated, the need for professionals who can design robust, holistic security architectures will increase. However, developing these skills typically requires years of experience, posing challenges for the short-term workforce; Legal Policy and Compliance Officers: These roles are becoming more critical as organizations navigate a complex legal landscape, including both national and international cybersecurity laws; Cyber Threat Intelligence Officers:

Although often incorporated into other roles within organizations, the need for dedicated threat intelligence officers will grow as cyber threats become more sophisticated; Cybersecurity Researchers: As cybersecurity threats evolve, research roles will become more significant for both government and private sector innovation.

Challenges in the current workforce show a noticeable skills gap between the training provided by educational institutions and the practical requirements of employers. Many companies cite difficulties in finding qualified candidates with real-world experience, even in entry-level roles. SMEs, in particular, face resource constraints, leading them to hire professionals who can manage multiple cybersecurity roles simultaneously. Larger organizations, though better positioned to hire specialists, also struggle to find candidates with the necessary advanced technical skills.

Recommendations for workforce development possibilities showcase training existing employees to handle emerging cybersecurity challenges is crucial. Many organizations emphasize the importance of continuous education to keep up with new technologies like AI and cloud security; Higher education institutions need to align curricula with market needs, incorporating hands-on experience through internships and practical labs. Certifications, especially in areas like cloud security and data protection, are becoming more important; There is a need for better cooperation between academia, industry, and government to address the gap between academic training and industry needs.

In conclusion, Estonia is actively addressing its cybersecurity workforce needs through education, national initiatives, and close collaboration between sectors. However, the demand for skilled professionals continues to outpace supply, especially for roles such as penetration testers, CISOs, and cybersecurity implementers. As threats evolve, the focus will shift towards more specialized roles, requiring continuous investment in both education and practical training to ensure Estonia remains a global leader in cybersecurity.

7.2 Skills for cybersecurity professionals

The skills required for cybersecurity professionals in Estonia, as identified through literature, expert panels, and surveys, reflect both the rapid technological advancements in the field and the pressing need to bridge the gap between education and industry requirements.

Technical Skills:

- Cloud Security and Data Privacy: As organizations adopt cloud services, securing cloud environments and ensuring data protection has become a critical skill set. Cloud security and cryptography were highlighted by both cybersecurity service providers and companies needing in-house expertise.
- Incident Response and Threat Analysis: Incident management skills, including the ability to analyze and respond to threats, are essential. Professionals must be proficient in forensic analysis, vulnerability assessments, and managing complex security environments, especially with evolving threats.
- Risk Management: Cybersecurity professionals must be skilled in assessing risks, conducting security assessments, and managing compliance with local and international frameworks, such as GDPR and ISO 27001.
- Secure Coding and Cryptography: Developing secure applications and understanding encryption standards (especially post-quantum cryptography) are emerging as crucial skills, as automation and AI-driven attacks evolve.

Non-Technical Skills:

- Analytical Thinking and Problem Solving: These skills are fundamental across all cybersecurity roles, enabling professionals to analyse complex situations, identify potential vulnerabilities, and find solutions to emerging threats.
- Communication and Collaboration: Given the increasing need for cross-departmental coordination, professionals must be able to explain technical issues to non-technical stakeholders and work effectively within diverse teams.

- Strategic Planning: For roles like Chief Information Security Officers (CISOs) and cybersecurity architects, long-term strategic planning is essential to align cybersecurity initiatives with broader business goals.
- Ethical Responsibility and Leadership: Leadership and ethical responsibility were emphasized, particularly in roles where professionals are responsible for handling sensitive data and making strategic decisions about an organization's cybersecurity framework.

Emerging Skills:

- AI and Machine Learning: The use of AI in both attacking and defending cybersecurity systems is increasing. Professionals must be prepared to secure AI-driven systems and utilize AI for defensive strategies.
- DevSecOps: Integrating security into the development process is becoming more important as organizations aim to streamline their operations while maintaining robust security measures.
- Challenges and Training Gaps:
- Lack of Hands-on Experience: Many cybersecurity graduates lack practical experience, resulting in a gap between the skills taught in educational institutions and those required in the workplace. This has made it difficult for companies to find qualified entry-level candidates.
- Upskilling and Reskilling Needs: Companies are increasingly focusing on upskilling their existing workforce, especially in cloud security, risk management, and threat analysis. Reskilling non-ICT personnel to foster a more security-aware workforce is also becoming a priority.
- Time Constraints in Training: Both cybersecurity service providers and companies cite time and resource constraints as significant barriers to continuous training, which limits their ability to keep up with the rapidly evolving threat landscape.

Recommendations to continue showcase the need of educational programs to incorporate more hands-on training, real-world problem-solving, and simulations to better prepare students for the cybersecurity challenges they will face in the workforce. Both formal education and non-formal training (such as certifications) must be emphasized to keep pace with new technologies like AI, cloud computing, and DevSecOps. Lifelong learning and modular training programs should be encouraged to help professionals remain adaptable in a dynamic field.

In summary, the cybersecurity workforce in Estonia must continually evolve, focusing on both technical expertise in emerging technologies and the non-technical skills necessary for leadership, problem-solving, and ethical responsibility. Addressing the current educational gaps through practical training, continuous learning, and industry collaboration is crucial for ensuring Estonia's cybersecurity professionals are equipped to handle future challenges.

7.3 Education and training of cybersecurity professionals

The findings from literature, expert panels, and questionnaires provide a comprehensive overview of the educational and training challenges faced by Estonia in developing a skilled cybersecurity workforce.

Educational Gaps:

- One of the most significant gaps identified is the lack of practical, hands-on experience in existing academic programs. Employers often express dissatisfaction with the skill levels of recent graduates, noting that they lack the practical knowledge needed for immediate impact in the workplace. This highlights a disconnect between academic curricula and industry needs, particularly for advanced roles like threat intelligence and incident response.
- Many programs provide a broad overview of ICT but fail to dive deep into specialized areas such as cloud security, advanced threat detection, or forensics. This leaves graduates underprepared for specialized roles that are increasingly important in Estonia's cybersecurity landscape.
- High dropout rates in ICT programs further exacerbate the skills shortage, reducing the pipeline of potential cybersecurity professionals.

Training and Upskilling:

- Upskilling ICT personnel within companies is a preferred method for bridging the skills gap. Both employers and experts agree that practical, real-time experience is vital for developing cybersecurity talent. On-the-job training and coaching are commonly used approaches to build the necessary skills.
- Given the limited supply of cybersecurity professionals, some companies have resorted to reskilling non-ICT staff to build internal cybersecurity awareness and practices, especially in roles related to data privacy and incident management.
- Lifelong learning is essential in the rapidly evolving cybersecurity field. Programs offering modular courses and stackable credentials enable professionals to keep pace with technological advancements, such as AI security and post-quantum cryptography.

Challenges in Training:

- Many professionals report that they are too busy managing ongoing threats to allocate time for training. Additionally, organizations often face difficulty in finding time and resources to organize adequate training programs.
- The cost of training programs is another significant barrier, particularly for smaller companies that struggle to afford external certifications or specialized training.
- There is a growing sentiment among employers that academia is not adequately aligned with the cybersecurity demands of the market. This results in a mismatch between the skills taught in educational institutions and those required in practice.

Recommendations for the next step means that academic programs must incorporate more practical elements, such as simulations, lab exercises, and internships, to better prepare students for the realities of cybersecurity roles. Collaborating with industry to offer internships and real-world projects would bridge the gap between theoretical learning and practical application; Combining online courses with in-person workshops would offer professionals the flexibility to balance work with continued education. These approaches can cover theoretical aspects through e-learning while focusing on practical training during in-person sessions; Educational institutions need to collaborate with industry experts to regularly update curricula to reflect emerging cybersecurity threats and technologies. Involving cybersecurity practitioners as guest lecturers or adjunct professors could help ensure that students are learning the most up-to-date skills; In Estonia, where many organizations require cybersecurity professionals to perform multiple roles, training programs should offer multi-disciplinary courses that combine elements of system administration, network security, and incident response.

In conclusion, while Estonia has made progress in developing cybersecurity education and training initiatives, addressing the current gaps in practical experience, specialization, and industry alignment is crucial. A stronger emphasis on real-world training, flexible learning opportunities, and close collaboration between academia and industry will ensure that Estonia can produce the next generation of cybersecurity professionals capable of meeting the country's growing cybersecurity needs.

8 References

1. CCDCOE (2013) The Cyber Defence Unit of the Estonian Defence League https://ccdcoe.org/uploads/2018/10/CDU_Analysis.pdf
2. Cyber/Ireland (2024) Learnings for Ireland from Estonia's Leadership in Cyber Security https://cyberireland.ie/learnings-for-ireland-from-estonias-leadership-in-cyber-security/
3. CyberSecPRo (2022) CyberSecPro - D2.1 Cybersecurity Practical Skills Gaps in Europe: Market Demand and Analyse state https://www.cybersecpro-project.eu/wp-content/uploads/2023/07/D2.1_Cybersecurity_Practical_Skills_Gaps_in_Europe_v.1.0.pdf
4. CyberSecPro Project. (2023). Cybersecurity Practical Skills Gaps in Europe. https://www.cybersecpro-project.eu/wp-content/uploads/2023/07/D2.1_Cybersecurity_Practical_Skills_Gaps_in_Europe_v.1.0.pdf
5. Defence Industry and Space (2024) EDF-funded EUROGUARD project kicks-off in Estonia https://defence-industry-space.ec.europa.eu/edf-funded-euroguard-project-kicks-estonia-2024-01-26_en
6. EAS (2022) Estonia supports 30 applied research and product development projects with 19.4 million euros https://eas.ee/en/estonia-supports-30-applied-research-and-product-development-projects-with-19-4-million-euros/
7. Education and Youth board (2024) IT Akadeemia infoturbejuhi koolitusprogramm https://harno.ee/it-akadeemia-infoturbejuhi-koolitusprogramm-0
8. Education Estonia. (n.d.). Overview of the Estonian education system. https://www.educationestonia.org/about-education-system/
9. e-Estonia. (2021). e-Estonia Programme for Cyber Security. https://e-estonia.com/programme/cyber-security/
10. e-Estonia. (2023). Advanced Cybersecurity Threats in Estonia. https://e-estonia.com/2023-estonia-advanced-cybersecurity-threats/
11. ENISA (2022) European Cybersecurity Skills Framework Role Profiles https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles
12. Estonia.ee (2021) Estonia ranks as the 3rd most secure country on the Global Cybersecurity Index https://estonia.ee/estonia-3rd-on-the-global-cybersecurity-index/
13. European Commission. (2020). Education and Training Monitor 2020: Estonia. https://op.europa.eu/webpub/eac/education-and-training-monitor-2020/countries/estonia.html
14. Fontes (2022) IT-sektori palgauuring https://palgauuringcms.fontes.ee/api/assets/portal/81ab707f-2b42-4fb0-80df-df607e3d8fdd/ikt-sektori-palgauuring-2022-eesti-kokkuvote.pdf
15. Fontes (2023) IT-sektori palgauuring https://palgauuringcms.fontes.ee/api/assets/portal/ec26e35b-b64c-44ee-99e6-ecd546a13323/ikt-sektori-palgauuring-2023-eesti-raport-kokkuvote.html
16. Haridussilm (2024) Smart Decisions with Haridussilm https://www.haridussilm.ee/
17. Information System Authority (2020a) Cyber Security in Estonia 2020 https://www.ria.ee/sites/default/files/documents/2022-11/Cyber-Security-in-Estonia-2020.pdf
18. Information System Authority (2020b) The 2020 yearbook of the Information System Authority https://www.ria.ee/sites/default/files/documents/2022-11/2020-yearbook-of-RIA.pdf
19. Information System Authority (2021) Cyber Security in Estonia 2021 https://www.ria.ee/sites/default/files/documents/2022-11/Cyber-Security-in-Estonia-2021.pdf
20. Information System Authority (2022) Cyber Security in Estonia 2022 https://www.ria.ee/sites/default/files/documents/2022-11/Cyber-Security-in-Estonia-2022.pdf
21. Information System Authority (2023) Cyber Security in Estonia 2023 https://www.ria.ee/sites/default/files/documents/2023-02/Cyber-Security-in-Estonia-2023.pdf
22. Information System Authority (2024a) Cyber Security in Estonia 2024 https://www.ria.ee/sites/default/files/documents/2024-02/Cyber-security-in-Estonia-2024.pdf
23. Information System Authority (2024b) Tehisintellekti ja masinõppe tehnoloogia riskide ja nende leevendamise võimaluste uuring https://www.ria.ee/sites/default/files/documents/2024-03/Tehisintellekti-masinoppe-tehnoloogia-riskide-uuring-2024.pdf
24. Information System Authority (2024c). Estonian information security standard (E-ITS)https://www.ria.ee/kuberturvalisus/riigi-infoturbe-meetmete-haldus/eesti-infoturbestandard-e-its
25. Information System Authority (2024d). RIA's Be Conscious! IT-vaatlik campaign. https://www.itvaatlik.ee/
26. Information System Authority (RIA). (n.d.). Küberpööre. https://www.ria.ee/kuberturvalisus/riiklik-koordinatsioonikeskus-ncc-ee/kuberpoore

27. International Telecommunication Union (ITU) (2024a) Estonia ranks fifth in the global cybersecurity index https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Estonia-ranks-fifth-in-the-global-cybersecurity-index.aspx
28. International Telecommunication Union (ITU) (2024b) Global Cybersecurity Index 2024 5th Edition https://www.itu.int/dms_pub/itu-d/opb/hdb/d-hdb-gci.01-2024-pdf-e.pdf
29. ITL (2022) Eesti IKT sektori teadus- ja arendustegevuse ülevaade ja vajadused https://etag.ee/wp-content/uploads/2022/09/EITL.pdf
30. ITL (2024) ITL launched a CyberTech Cluster https://itl.ee/en/news/itl-launched-a-cybertech-cluster/
31. Kohler, K (2020) Estonia's National Cybersecurity and Cyberdefense Posture Center for Security Studies (CSS), ETH Zurich https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-09-Estonia.pdf
32. Kutsekoda. (2022a). OSKA IKT 2021 Overview. https://oska.kutsekoda.ee/wp-content/uploads/2022/01/OSKA_IKT_2021_terviktekst_.pdf
33. Kutsekoda. (2022b). OSKA IKT Study: Future Trends in Estonia's ICT sector. https://uuringud.oska.kutsekoda.ee/uuringud/info-kommunikatsioonitehnoloogia
34. Kutsekoda. (2022c.). OSKA trendikaardid. https://oska.kutsekoda.ee/trendid/
35. Laasmäe, H (2011) Estonia: Cyber Window into the Future of NATO Ndupress.ndu.edu https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-63/jfq-63_58-63_Laasme.pdf?ver=Gmp2P_MaR_5WUw4ETKCnXA%3D%3D
36. Ministry of Economic Affairs and Communication (2014) Cyber Security Strategy 2014-2007 https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Estonia_Cyber_security_Strategy.pdf
37. Ministry of Economic Affairs and Communications. (2018). Cybersecurity Strategy Republic of Estonia 2019-2020. https://www.mkm.ee/media/703/download
38. Ministry of Economic Affairs and Communications. (2024). Kyberturvalisuse strateegia 2024-2030. https://www.mkm.ee/sites/default/files/documents/2024-07/Kyberturvalisuse%20strateegia%202024-2030_labivalt_IT_vaatlik_Eesti.pdf
39. Ministry of Foreign Affairs of Estonia. (2024). Cybersecurity in Estonia. https://vm.ee/sites/default/files/documents/2024-03/Cyber_0.pdf
40. NCSI (2024) National security index: Estonia https://ncsi.ega.ee/country/ee/
41. OECD. (2023). Education at a Glance: Estonia. https://gpseducation.oecd.org/Content/EAGCountryNotes/EAG2023_CN_EST_pdf.pdf
42. Pernik, P (2021) Cyber deterrence: A case study on Estonia's policies and practice. Hybrid CoE https://www.hybridcoe.fi/wp-content/uploads/2021/10/20211012_Hybrid_CoE_Paper_8_Cyber_deterrence_WEB.pdf
43. Praxis (2019) Küberturbe valdkonna tööjõuvajaduse ja hariduse uuring https://www.praxis.ee/uploads/2018/04/K%C3%BCberturbe-uuring_aruanne-23_04_2019.pdf
44. Praxis (2023) Sekkumised avalik sektori IT-oskuste arendamisel https://www.praxis.ee/tood/sekkumised-avaliku-sektori-it-oskuste-arendamisel/
45. Riigiteataja. (2019). Consolidated legislation: Cybersecurity. https://www.riigiteataja.ee/en/eli/523012019001/consolide

Co-funded by
the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.