REWIRE
Cybersecurity Skills Alliance

Co-funded by the
Erasmus+ Programme
of the European Union

**REWIRE -** Cybersecurity Skills Alliance
A New Vision for Europe

# R5.2.1 Second Annual Cybersecurity Skills Trends Report

| | |
|---|---|
| **Title** | R5.2.1 Annual Cybersecurity Skills Trends Reports |
| **Document description** | 2nd Annual Cybersecurity Skills Trends Report within R5.2.1 |
| **Nature** | Public |
| **Task** | T5.2.1 Annual Cybersecurity Skills Trends Reports |
| **Status** | Updated version |
| **WP** | WP5 |
| **Lead Partner** | MRU |
| **Partners Involved** | All |
| **Date** | 21/11/2024 |

# CONTENTS

# LIST OF ABBREVIATIONS AND ACRONYMS

| Abbreviation | Explanation/ Definition |
|---|---|
| ACSC | Australian Cyber Security Centre |
| CISO | Chief Information Security Officer |
| DDoS | Distributed Denial of Service |
| DoS | Denial of Service |
| ENISA | The European Union Agency for Cybersecurity |
| EU | The European Union |
| ECSF | European Cyber Security Framework |
| GDPR | General Data Protection Regulation |
| IoT | Internet of Things |
| MITM | Man-in-the-Middle |
| NCSC | National Cyber Security Centre (New Zealand) |
| PhaaS | Phishing-as-a-Service |
| RaaS | Ransomware as a Service |
| RDoS | Ransom Denial of Service |
| RFID | Radio-frequency identification |

*Table 1. List of abbreviations and acronyms*

# LIST OF TABLES

# LIST OF FIGURES

## SUMMARY

This deliverable is an integral component of an overarching aim of REWIRE to monitor, report, and evaluate the state of cybersecurity skills within the EU, offering a yearly snapshot of the identified cybersecurity skills gaps. Its scope is comprehensive, aimed at illuminating the landscape of cybersecurity expertise – from the trends in the cybersecurity workforce to the emergence of new skill sets. The report seeks to provide a better understanding of overall situation in cybersecurity skills market. It is positioned to serve as a critical resource for stakeholders at various levels providing them with the intelligence needed to make informed decisions and strategic adjustments.

The analysis of the skills market is a cornerstone of this report. It is not merely an assessment of the current availability of skills but a prognostic tool that highlights where the sector falls short and where it must evolve. Moreover, the report offers a detailed examination of the prevailing cybersecurity threat trends that have been observed over the past year. This examination is not conducted in isolation; it correlates these trends with workforce competencies, thereby providing a clearer picture of how the skills available in the market align with the threats encountered.

In essence, this deliverable serves as a strategic tool, a call to action, and a beacon for future readiness. It underscores the importance of adaptive education, proactive policy-making, and strategic workforce development to ensure that the cybersecurity sector remains robust, agile, and capable of withstanding the ever-evolving threats that it faces.

# 1. INTRODUCTION

In an environment where cybersecurity dynamics are in constant flux, a structured approach to tracking and analyzing trends is crucial. The 2nd Annual Cybersecurity Skills Trends Report, crafted by the Erasmus+ REWIRE project, represents a concerted effort to systematically gather data on the shifting landscape of cybersecurity competencies. The aim is to identify and anticipate future needs in the cybersecurity skill sector, laying a foundation for the development of subsequent project deliverables.

The structure of the Report is meticulously organized into several key sections:

Section 2 outlines the methodology employed by REWIRE to track and analyze trends in cybersecurity skills. This methodological framework is critical for ensuring that the data collected is robust and that the analysis is grounded in a repeatable, scientific approach.

Section 3 offers an in-depth examination of the current cybersecurity skills demand landscape. It meticulously articulates the findings and insights gleaned from the Cybersecurity Job Ads Analyzer and the stakeholder survey, both of which are instrumental in pinpointing existing skills gaps and assessing the state of cybersecurity competencies across the industry.

Section 4 offers an analysis of cybersecurity threat trends. By understanding the trajectory of threats, one can infer the direction in which cybersecurity skills need to evolve to counteract these threats effectively.

Finally, Section 5 encapsulates the essence of the report by merging the identified cybersecurity threats with the requisite skills necessary for their mitigation. This synthesis informs curriculum development, training programs, and policy-making. It ensures that educational institutions, training providers, and policymakers are in lockstep with the practical needs of the cybersecurity realm, equipping professionals with the tools and knowledge to safeguard digital assets in an increasingly complex and vulnerable cyber landscape.

This report builds on the foundation laid by the initial report delivered in October 2022 and will be further expanded in the forthcoming report in October 2024. By maintaining a pulse on the sector's progression, the REWIRE project ensures that its outputs remain relevant and that stakeholders are equipped with the knowledge to make informed decisions in the rapidly evolving cybersecurity domain.

# 2. METHODOLOGY

To construct this report, the project team used diverse information sources. The list in Table 2 depicts the information sources used or planned to be used in the future to support the creation of this report and its iterations.

| Information source | Description | Status and Periodicity |
|---|---|---|
| Stakeholders' survey | The Survey conducted to collect information about unfilled cybersecurity job positions, the most sought-after skills and the ability of education providers to train the needed professionals | In progress – will be provided in the third report<br><br>First results in 2021 – reported in R2.2.2. Cybersecurity Skills Needs Analysis and in 1st Annual Cybersecurity Skills Trends Report within R5.2.1<br><br>Repeated every two years |
| Job Ads Analysis | This tool created by REWIRE team allows identifying, which cybersecurity skills are required within an ad and creates appropriate mappings to the relevant cybersecurity roles | Implemented<br><br>(2023)<br><br>(First results in 2022)<br><br>Repeated annually |
| National, regional, European and industry risk and threat reports | Cybersecurity risk and threats reports of various actors (e.g., ENISA), governmental reports (UK, New Zealand, Australia, etc.) and similar are reviewed to provide insights on the subjects of cybersecurity skills. | Implemented<br><br>(2023)<br><br>Repeated annually |
| Sectoral surveys and studies | Sectoral surveys and studies from various organizations (e.g., CrowdStrike, Sophos, Truesec, etc.) are reviewed in order to provide further insights on the subjects of cybersecurity skills | Implemented<br><br>(2023)<br><br>Repeated annually |
| The CyberABILITY platform | The CyberABILITY platform will combine information and present information to interested parties on the 12 roles of the ECSF, | In progress – will be provided in the third report4 |

| Information source | Description | Status and Periodicity |
|---|---|---|
| | professional courses, academic degrees and certifications. | |

***Table 2. Skills Trend Report information sources***

The initial methodological approach included two steps. First, a Stakeholders' survey to be conducted in order to identify the most coveted skills and the capacity of educational institutions to educate the required professionals. Second, results of Job Ads Analysis that enabled the recognition of certain skills necessitated in respective ads and established corresponding links to the pertinent roles in cybersecurity. Due to limited possibilities to gather reasonable responses from the stakeholders (e.g.: privacy issues, absence of EU level recognised skills framework, time constrains, complexity of the issue, etc.) it was decided to include the results of the stakeholders survey in the third report and instead supplement this methodological step with extensive review of different secondary sources that reflect the skills related issues in cybersecurity for this report. Comparative analysis of different sectoral surveys and studies as well as the national threats trends reports is conducted in this report to identify the latest cybersecurity threats trends which emerged over the last year. It then allows the analysis of the respective skills required to tackle the emerging threats. For each skills trend report, the information derived from all these sources and any new identified at that time will be combined to produce the relevant insights. The following Section 3 provides more information on the implementation of the methodology.

In the expert evaluation of this report, it was noted that "the evolution in the education landscape makes the findings of previous projects obsolete. While the methodologies proposed in those projects are still relevant, their conclusions should be left in favour of the analysis of the current scenario. This is one of the weak points of the version of R.5.2.1 released in March 2023. The version of the same report released in December 2023 does not reference the results of old projects, but in the tentative of making the document aligned with current threats, it missed the original methodological framework." In response to these observations, the starting point for the First Annual Cybersecurity Trends Report was the study of the information, deliverables, and activities of the pilot projects to gain their perspective on emerging cybersecurity skills. As intended, since the pilot projects' results were already presented, they were not included in the Second Annual Cybersecurity Trends Report. Thus, it should be emphasized that the methodology has been intentionally changed and should not be considered a methodological drawback.

# 3. STATUS OF CYBERSECURITY SKILLS AND SYSTEMATIC SKILL GAPS: JOB ADS ANALYSIS

In the second annual report the REWIRE partners embark the following approach to elucidate the landscape of the cybersecurity skills shortage, mainly the **Development of the Cybersecurity Job Ads Analyzer.** This innovative application is designed as a tool to aggregate and examine job adverts. It incorporates a machine learning algorithm, which is instrumental in pinpointing and delineating the specific competencies sought in an advertised open cybersecurity job market. The analysers' sophisticated capabilities enable a granular analysis of the evolving demands of cybersecurity skills, thus providing invaluable insights into the current skills ecosystem. The insights developed via Job Ads Analysis will be integrated within the CyberABILITY platform presenting the fuller picture of the skills required to respond to certain threats.

The subsequent section will offer a description of this measure, outlining the methodology employed, the data gathered, and the analytical frameworks applied. The findings and implications drawn from both the Cybersecurity Job Ads Analyzer is pivotal, not just for understanding the current state of cybersecurity skills requirements, but also for shaping future strategies to bridge the gap effectively.

Taking as a starting point the work performed as part of the R.2.2.3. *Methodology to anticipate future needs* and R2.2.2 *Cybersecurity Skills Needs Analysis*, the REWIRE project has developed and further evolved a dynamic web application called *Cybersecurity Job Ads Analyzer*[i]. This tool allows identifying which cybersecurity skills are required in a work role.

The Cybersecurity Job Ads Analyzer is not merely a standalone application but a key component of the greater REWIRE R5.1 CyberABILITY platform.

The following diagram (see Figure 1) depicts the main components and characteristics of the Job Ads Analyzer tool:

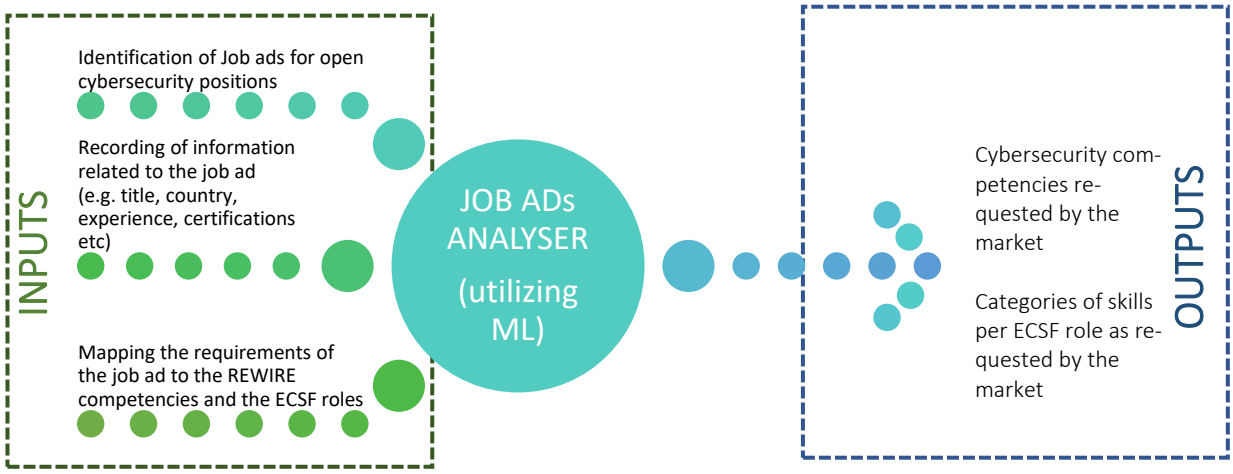


*Figure 1. Process diagram of the Job Ads Analyser tool*





REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

The tool has four main views: 1) the database, 2) the "Create Your Ad" tab, 3) the "Statistics" tab, and 4) the Machine Learning (ML) Algorithms. The Job Ads Analyzer allows users to add job adverts. Filters can be applied based on various parameters such as the country of the job posting, the year it was posted, allowing for a tailored search experience. The ML algorithm permits analysing a selection of ads depending on the chosen filtering. For instance, a user can select all the ads related to the ENISA Cybersecurity Architect profile, process them through the ML algorithm, and obtain which skills are the most needed for this profile.

The Job Ads Analyzer has revealed a compelling set of data that reflects the contemporary landscape of the cybersecurity job market. The top 10 skills, according to its findings, illustrate a blend of soft skills, technical expertise, and strategic acumen that are in high demand across the industry.

List of the 10 most sought-after skills (for medium dataset)

| Rank | Skill | Occurrence |
|---|---|---|
| 1 | Collaborate and Communicate | 85.28 % |
| 2 | Information Systems and Network Security | 67.41 % |
| 3 | Information Security Controls Assessment | 65.05 % |
| 4 | Business Continuity | 50.2 % |
| 5 | Risk Management | 49.41 % |
| 6 | Threat Analysis | 48.75 % |
| 7 | Organizational Awareness | 48.62 % |
| 8 | Incident Management | 46.65 % |
| 9 | Data Security | 45.07 % |
| 10 | Enterprise Architecture and Infrastructure Design | 44.55 % |

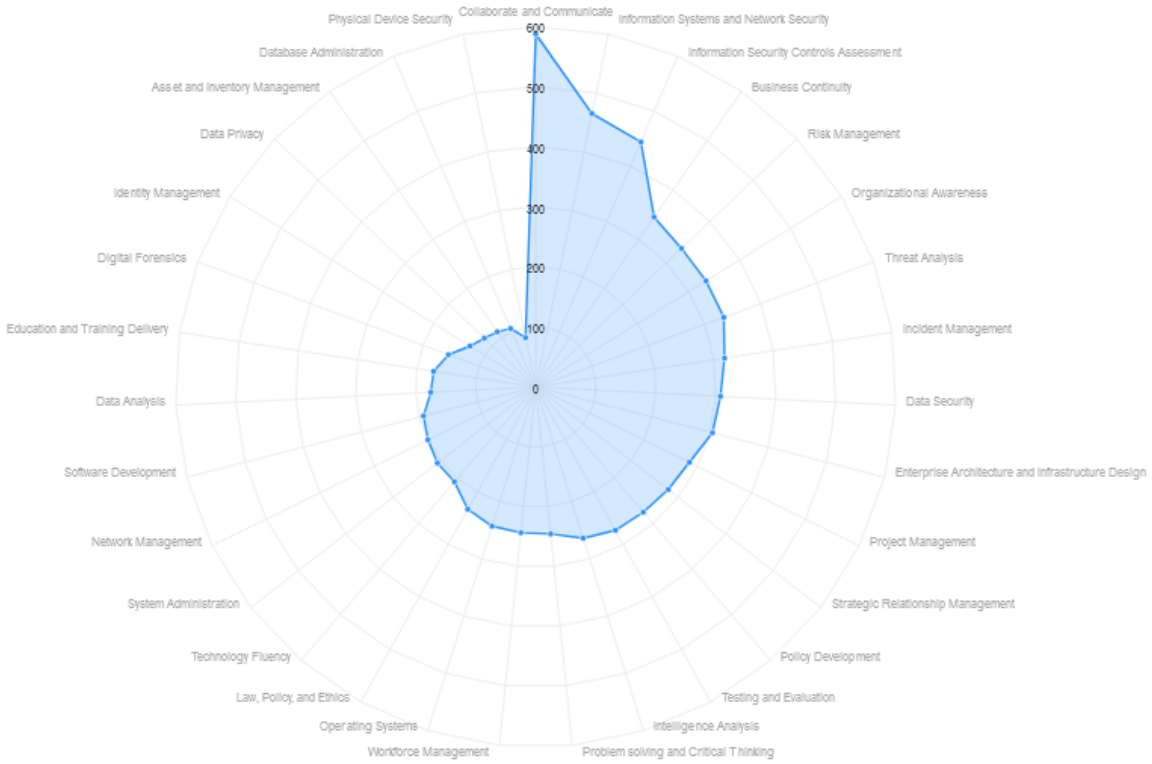


***Figure 2. Top 10 identified cybersecurity skills in the database***

At the moment of the submission of this deliverable, the Job Ads Analyzer counted 927 inserted jobs. Specifically, the ads were categorized based on ENISA profiles (see Table 3).

| **ENISA profile** | **Number of Ads** |
|---|---|
| Chief Information Security Officer | 99 |
| Cybersecurity Architect | 142 |

| | |
|---|---|
| Cybersecurity Auditor | 75 |
| Cybersecurity Educator | 18 |
| Cybersecurity Implementer | 148 |
| Cyber Incident Responder | 115 |
| Cyber Legal, Policy & Compliance Officer | 53 |
| Cybersecurity Researcher | 44 |
| Cybersecurity Risk Manager | 76 |
| Cyber Threat Intelligence Specialist | 57 |
| Digital Forensics Investigator | 22 |
| Penetration Tester | 69 |

***Table 3. Number of Ads***

It is important to note that each ad can be linked to more ENISA profiles. The above table shows the connection to the main identified profile.

For the REWIRE project, particular attention is given to several specialized roles—Chief Information Security Officer (CISO), Cyber Threat Intelligence Specialist, Cyber Incident Responder, and Penetration Tester. These roles are earmarked for deeper analysis in terms of developing dedicated trainings and certification schemes, recognizing their pivotal position within the cybersecurity ecosystem. The selection of these profiles for the REWIRE project is grounded in criteria, detailed in the R4.2.1 *REWIRE Curricula and Training Framework* and other documented sources[ii].

For the CISO, the identified skills with the respective occurrences are shown in Table 4.

| Rank | Skill | Occurrence |
|---|---|---|
| 1 | Collaborate and Communicate | 56 % |
| 2 | Threat Analysis | 46 % |
| 3 | Data Security | 41 % |
| 4 | Information Systems and Network Security | 31 % |
| 5 | Risk Management | 24 % |
| 6 | Testing and Evaluation | 19 % |
| 7 | Operating Systems | 16 % |
| 8 | Incident Management | 12 % |
| 9 | Business Continuity | 12 % |
| 10 | Information Security Controls Assessment | 11 % |
| 11 | Project Management | 9 % |
| 12 | Software Development | 6 % |
| 13 | Law, Policy, and Ethics | 6 % |
| 14 | Organizational Awareness | 6 % |

| Rank | Skill | Occurrence |
|---|---|---|
| 15 | Intelligence Analysis | 6 % |
| 16 | Enterprise Architecture | 6 % |
| 17 | Data Analysis | 3 % |
| 18 | Identity Management | 1 % |
| 19 | System Administration | 1 % |
| 20 | Policy Development | 1 % |

***Table 4. Skills for CISO profile***

Table 5 presents a side-by-side comparison of the top 10 skills as they appear in the general pool of job advertisements versus those specifically associated with the Chief Information Security Officer (CISO) role. The skills shared between the two columns are highlighted with the same color to denote overlap, indicating their relevance across the wider cybersecurity job market as well as their particular importance to the CISO position.

For the general ads, the skill 'Collaborate and Communicate' appears at the top, followed by a list that leans towards technical expertise such as 'Information Systems and Network Security', and 'Information Security Controls Assessment'. 'Business Continuity' and 'Threat Analysis' also feature prominently, reflecting a balanced mix of strategic and operational capabilities.

In the CISO-specific column, 'Collaborate and Communicate' again leads the list, underlining the critical nature of communication skills for leadership roles. 'Threat Analysis' and 'Data Security' are notably higher on the CISO list than in the general ads, which may reflect the strategic risk management responsibilities of the CISO. Other skills such as 'Testing and Evaluation', and 'Operating Systems' are unique to the CISO profile in terms that these skills do not appear among the top 10 skills in the general pool of job advertisements, highlighting the hands-on technical knowledge that is expected of a CISO, in addition to their management duties. The overlaps, particularly in 'Incident Management' and 'Business Continuity', underscore that while the CISO is a leadership role, it still demands a firm grasp of the technical and operational aspects of cybersecurity.

| All Ads | CISO ads |
|---|---|
| Collaborate and Communicate | Collaborate and Communicate |
| Information Systems and Network Security | Threat Analysis |
| Information Security Controls Assessment | Data Security |
| Business Continuity | Information Systems and Network Security |
| Threat Analysis | Risk Management |
| Risk Management | Testing and Evaluation |
| Organizational Awareness | Operating Systems |
| Incident Management | Incident Management |





REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

| | |
|---|---|
| Data Security | Business Continuity |
| Enterprise Architecture and Infrastructure Design | Information Security Controls Assessment |

*Table 5. Top 10 skills: all adds v. CISO ads*

To conclude, the REWIRE's dual strategy, using the Job Ads Analyzer and Stakeholders' survey, has produced important insights for better understanding of overall situation in cybersecurity skills market. By aligning with established skills frameworks and role profiles, REWIRE has effectively mapped the current and future needs of the cybersecurity workforce. The data derived from these tools is crucial for shaping targeted educational and professional development initiatives, ensuring the cybersecurity sector meets emerging challenges with a well-equipped and proficient workforce.

# 4. CYBERSECURITY THREATS TRENDS

This chapter aims to conduct a comparative analysis of different sectoral surveys and studies as well as the national threats trends reports to identify the latest cybersecurity threats trends which emerged over the last year. It is important to track the emerging threats in order to be able to react and adapt the respective cybersecurity skills necessary to the new trends.

The ENISA Threat Landscape report of 2023 (ENISA report) indicates that the primary threats identified in 2022 remain the same.[iii] The prime threats identified due to their prominence over the reporting period are ransomware, malware, social engineering, threats against data, threats against availability and integrity, disinformation – misinformation, and supply-chain attacks.

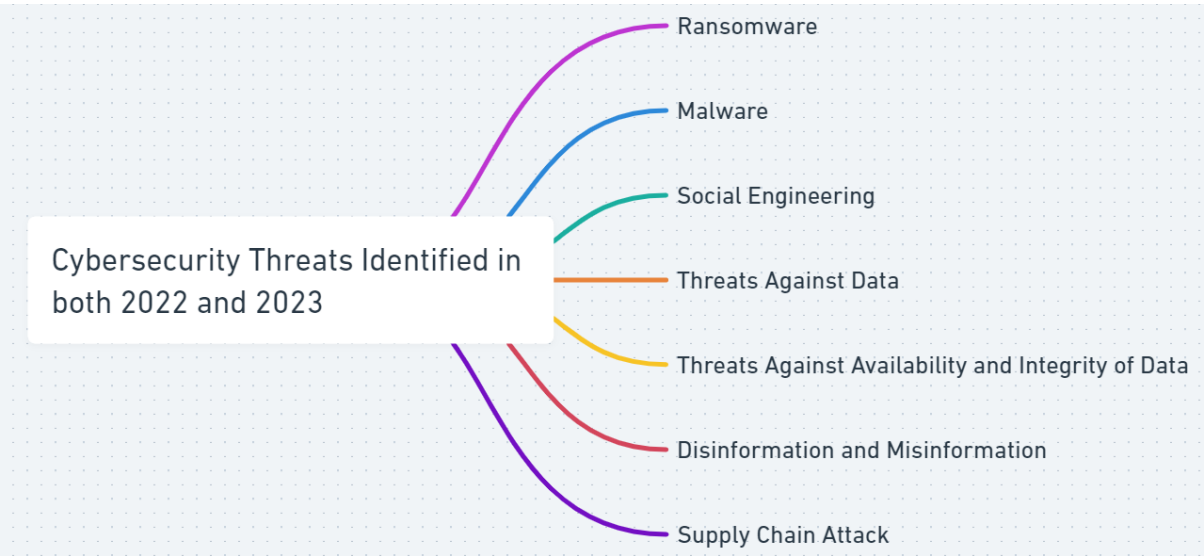


***Figure 3. Cybersecurity Threats Identified in both 2022 and 2023***

**Ransomware** remains the main cybersecurity threat globally. According to ENISA, it ranked at the top during the reporting period (31,32 percent of reported incidents).[iv] ENISA defines ransomware as a type of attack where threat actors take control of a target's assets and demand a ransom in exchange for the return of the asset's availability. This broad definition encompasses the evolving landscape of ransomware threats, the widespread use of diverse extortion methods, and the variety of objectives of the perpetrators, which extend beyond merely financial gains.[v] UK NCSC indicates that ransomware is an illicit commercial enterprise – an evolving threat as the criminals chase the best ways to make money. During previous years, ransomware principally threatened to block organisations from accessing their systems through encryption. Currently, the UK NCSC is progressively observing data extortion as a substantial part of the ransomware business model as criminals understand that organisations are willing to pay to prevent the leaking of their data.[vi] The ACSC assessed that ransomware continue to be the most destructive cybercrime threat. Ransomware directly affected every sector of the Australian economy in the previous fiscal year.[vii] As reported by Truesec 2023, cybercrime is an international issue, with cybercriminals capable of launching attacks

from any location. Ransomware continues to be the foremost cyber threat facing organizations. This encompasses a range from broadly disseminated, automated ransomware campaigns to "big game hunting" attacks, wherein teams of skilled cybercriminals manually target organizations with precision attacks.[viii]

*Ransomware numbers*. According to UK NCSC, ransomware is one of the most significant cyber security threats facing businesses and organisations in the UK. Successfully deployed ransomware can potentially prevent public services and businesses from operating and putting their data at significant risk. Last year the UK NCSC coordinated the national response to 18 ransomware attacks including the attacks on a supplier to NHS 111, and South Staffordshire Water. However, the actual count of ransomware attacks in the UK annually is significantly greater, since many organizations frequently fail to report these breaches.[ix] The UK NCSC observes that there had been an increase in sophisticated, high-impact ransomware incidents against critical infrastructure organisations globally. Due to its potential impact on critical national infrastructure and essential services, ransomware is regarded as a national security risk.[x] As ACSC observed, leading ransomware groups persist in targeting Australian 'big game' entities – those that are high-profile, high-value, or critical service providers. Although global trends show a decrease in targeting such 'big game' entities and a shift towards smaller and medium-sized businesses, this trend has not yet become evident in Australia.[xi]

In Australia, the ACSC received 447 ransomware cybercrime reports. Although this represents a 10 percent reduction from the 2020–21 fiscal year, the reports still exceed those in 2019–20. Additionally, it's probable that ransomware incidents are considerably underreported, particularly by victims who opt to pay the ransom.[xii] In 2021–22, the education and training sector reported the highest number of ransomware incidents, up from being the fourth most reported sector in 2020–21. The risk to this sector is considerable due to its business model, which emphasizes open, collaborative environments.

Additionally, the shift to remote learning during the coronavirus pandemic led to the introduction of numerous personal devices and new software into the sector.[xiii] Overall, during the 2021–22 financial year, the top 5 sectors reporting ransomware incidents comprised 47 percent of all ransomware-related cybercrime reports. [xiv] Consequently, the ACSC addressed 135 cyber security incidents connected to ransomware, marking an increase of over 75 percent compared to the 2019–20 period. In addition, the ACSC identified and notified 148 organisations of ransomware activity. [xv]

In 2023, Truesec noted a decrease in ransomware attacks among our clients during the first half of 2022. This decline occurred as cybercriminals restructured some of their financial operations in response to the Russian invasion of Ukraine and ensuing sanctions. However, this impact was short-lived; in the latter half of 2022, Truesec estimated a 25% increase in ransomware incidents compared to the prior year.[xvi]

*Ransomware payment dynamics*. The UK NCSC suggests that ransom payment motivates harmful actions by perpetrators and does not ensure networks' decryption or give back taken data.[xvii] According to ACSC, ransomware victims still used third-party negotiators to facilitate payment of ransom demands in 2021–22. The extent of coverage offered by cyber insurance policies also plays a role in how victims handle and resolve these incidents and in a business's

decision on whether to pay the ransom.[xviii] A 2022 Australian Institute of Criminology study revealed that only 19 percent of ransomware victims turned to the police or the ACSC for advice or support. However, the research indicated that nearly 60 percent sought assistance from at least one formal source beyond their family or friends. The study also showed that 23.2 percent of small to medium business victims paid the ransom, resulting in the payment of millions of dollars in ransoms and related expenses.[xix] As reported by Sophos 2023, ransomware groups are also looking into broader ways to diversify their operations. A prime instance of this is the expansion of leak sites, where attackers publicize information about their victims. Historically, the model has been straightforward: if organizations pay the ransom, their data isn't posted on the leak site; if they don't pay, it is. However, this year has witnessed some intriguing evolutions in this area.[xx]

*Ransomware as a Service (RaaS).* The UK NCSC observed an increased use of Ransomware as a Service (RaaS) where less-skilled affiliates can rent different types of ransomware, enabling them to execute cyber-attacks without having to create the ransomware on their own. This expansion allows a broader spectrum of criminal actors to access the ransomware attack method, previously limited to individuals with the necessary technical skills. The UK NCSC noted that although reports in May 2022 indicated the discontinuation of the Conti ransomware strain, by August of the same year, this had not resulted in a decreased ransomware threat to the UK. This was because some members of the organized crime group responsible for Conti shifted to other ransomware groups. Consequently, the UK NCSC anticipates a more varied and potent ransomware environment.[xxi] The ACSC noted the rise of new and potentially rebranded RaaS operations throughout 2021–22. The presence of RaaS options provides cybercriminals with a variety of tools to choose from. Additionally, ransomware syndicates have further professionalized by employing third parties to negotiate with victims, facilitate the receipt of ransom payments, and resolve disputes among actors. [xxii]

In addition, according to ACSC, the business model of ransomware groups has continued to develop. Now, some of these groups are sharing information about their victims, amplifying the ransomware threat as victims may face attacks from multiple groups. For instance, following its closure announcement, the BlackMatter group handed over its victims to the ransomware infrastructure of another group, Lockbit 2.0. Additionally, in October 2021, members of the Conti ransomware group were reported to have started selling access to their victims' networks, allowing subsequent targeting by other entities.[xxiii]

In 2021–22, ransomware actors persisted in integrating extra extortion methods into their activities to more efficiently secure payments from victims. ACSC noted that the tactic of using both data encryption and threats to disclose sensitive information publicly to coerce ransomware victims into paying is termed 'double extortion'. Victims who might have previously recovered from a ransomware attack through regular backups can still be susceptible to reputational harm due to 'double extortion'. This is referred to as 'multifaceted extortion'. Additional extortion tactics used include persuading third-party stakeholders to pressure victims into negotiations and conducting continuous DDoS attacks on the victim's network during ransom negotiations. [xxiv]

According to CrowdStrike 2023, throughout 2022, perpetrators consistently demonstrated their capacity to adapt, fragment, regroup, and thrive despite defensive strategies. Following

the shutdown of some of the largest and most infamous ransomware enterprises, affiliates transitioned to new Ransomware-as-a-Service (RaaS) operations. Moreover, over 2,500 advertisements for access were discovered across the criminal underground, marking a 112% increase from 2021 and clearly indicating a growing demand for access broker services.[xxv] As noted by Sophos 2023, although there has been some disruption of ransomware groups in the past year due to factors such as geopolitical unrest and occasional prosecutions, new groups have emerged from the remnants of old ones, and ransomware activity continues to be one of the most widespread cybercrime threats to organizations. Ransomware operators are persistently evolving their methods and mechanisms, aiming to avoid detection and integrate new techniques.[xxvi]

As reported by Sophos 2023, Several ransomware groups have started utilizing new programming languages to complicate detection efforts, to enable easier compilation of the ransomware executable across various operating systems or platforms, or simply because the malware developers are skilled in these languages and tools. For example, BlackCat and Hive ransomware developers have adopted the Rust programming language, whereas the malware from BlackByte is written in Go (also known as GoLang).[xxvii] In addition to diversifying the programming languages used, ransomware has also altered its targeting strategy, moving beyond solely focusing on Windows systems. RedAlert, or N13V, targets both Windows and Linux ESXi servers, similar to Luna, another ransomware strain based on Rust. However, it's not just lesser-known groups making these changes; researchers discovered a Linux-ESXi variant of the prominent LockBit ransomware at the beginning of the year. These shifts in targeted platforms open up more opportunities for threat actors – expanding the attack surface, increasing pressure on victims, and potentially reducing the risk of detection, especially since the majority of anti-ransomware defences are primarily focused on Windows.[xxviii] Groups like Karakurt and AvosLocker have also adopted this trend, setting up auctions for stolen data. Others, like Snatch, are considering shifting their leak disclosures to a subscription model. Some sites are adding a new dimension to post-disclosure processes; if a victim pays, not only is their information kept private, but even the occurrence of the breach itself remains undisclosed. Suppose the breach has already been announced on leak sites. In that case, that mention is removed upon payment – potentially implicating the victim in hiding incidents that, in many countries, are legally required to be reported to regulators.[xxix]

According to Truesec 2023, modern ransomware syndicates have evolved into organized businesses. Truesec and the broader cybersecurity community have frequently labelled ransomware criminals as "gangs," but this term might not accurately reflect their nature. Structurally, major ransomware syndicates resemble contemporary tech startups more than traditional street gangs. This enhanced organization leads to specialization. Actors within ransomware ecosystems often focus on specific skills and trade or lease their expertise and tools to others within an extensive criminal economy.[xxx] In examining the primary attack methods employed in serious ransomware incidents, Tuesec noticed that the three most prevalent vectors continue to be the same as in 2021: phishing emails, vulnerability exploits, and the use of valid credentials for remote services like VPNs and RDP (Remote Desktop Protocol).[xxxi]

Yet, the most significant shift observed in 2022 compared to 2021 was the increased use of valid credentials to infiltrate organizations. This trend aligns with the swiftly expanding

market of Initial Access Brokers (IABs) – cybercriminals specialising in stealing credentials and selling them to other cybercriminals, including ransomware groups. Implementing multifactor authentication (MFA) should be a compulsory measure. However, it's noteworthy that some IABs have started providing services to bypass MFA by utilizing stolen tokens.[xxxii]

*Ransomware and Russia*. Most ransomware criminal groups targeting the UK are based in and around Russia, UK NCSC noticed. While the degree to which the Kremlin controls these ransomware groups is not clear, individuals operating within Russia's borders enjoy implicit approval from the Russian State.[xxxiii] Sophos 2023 reported, that observed a few lesser-known ransomware or leak groups that appear to be politically motivated, unlike some of their more notorious counterparts. One such example is a leak site focused on distributing materials from breaches involving Ukrainian citizens and government organizations. However, the source of this data and whether ransomware plays a role in its acquisition remains unclear.[xxxiv]

In turn, the New Zealand NCSC observed less high-impact ransomware and distributed denial-of-service (DDoS) activities in 2021/2022 than in 2020/2021. Possibly, the decrease in ransomware and DDoS attacks targeting New Zealand during 2021/2022 is linked to Russia's invasion of Ukraine. The invasion has undoubtedly disturbed cyber criminals operating in Russia and Ukraine, probably leading them to shift their strategic goals. The noted decrease in ransomware aligns with global trends seen in early 2022, DDoS activity has been more turbulent before and after Russia's invasion of Ukraine. DDoS activity surged in several countries, such as Ukraine, Russia, and various nations opposing Russia's invasion of Ukraine, while it declined in other areas.[xxxv]

The majority of cybercrime incidents addressed by Truesec are traced back to cybercriminals based in Russia. Ransomware, especially, is closely linked to the Russian cybercrime ecosystem.[xxxvi]

**Malware** is another significant category of threats distinguished by the majority of reports. According to ENISA, it comprised a significant part of incidents over the reporting period (8,24 percent of reported incidents).[xxxvii] Malware, also called malicious code and logic, is an overarching term used to describe any software or firmware intended to perform an unauthorised process that will adversely impact the confidentiality, integrity or availability of a system.[xxxviii]

According to UK NCSC, malware is a low sophisticated cyber security threat that most British public are likely to experience. Cyber criminals deploy commodity attacks, such as phishing or malware with the aim of scamming the public and businesses.[xxxix] Yet, as observed by CrowdStrike, there was a continued shift away from malware use, with malware-free activity accounting for 71% of all detections in 2022 (up from 62% in 2021). This situation was partly due to adversaries' extensive use of valid credentials to gain and maintain access in victim environments. Another contributing factor was the frequency of new vulnerabilities being disclosed and the speed with which adversaries could operationalize the exploits.[xl]

As noted by ACSC, cyberspace is increasingly the domain of warfare, as seen in Russia's use of malware designed to destroy data and prevent computers from booting in Ukraine. Russia was not the only nation leveraging cyber operations to advance its strategic interests. [xli] CrowdStrike reported, that on February 23, 2022, just within 48 hours, new wiper malware

variants such as *DriveSlayer*, *PartyTicket*, *IsaacWiper*, and *AcidRain* were unleashed against specific networks, aligning with the onset of Russia's military invasion in the early hours of February 24, 2022. The use of *AcidRain* was particularly significant, occurring less than an hour after Russian President Vladimir Putin announced the "special military operation." This malware seemed tailor-made to target and disrupt segments of the Viasat satellite communications network, which was crucial for providing network connectivity in Ukraine. The full extent of this early strike against Ukrainian government and military communications systems is still somewhat ambiguous, but its effects extended beyond Ukraine's borders. The disruption impacted at least three internet service providers across Europe, leading to service outages for thousands of customers and affecting the network communications of wind turbines in certain regions of Germany.[xlii]

In July 2021, the Australian Government openly attributed the exploitation of Microsoft Exchange vulnerabilities to China's Ministry of State Security. Additionally, a joint advisory from the Five-Eyes intelligence alliance in November 2021 confirmed that an Iranian state actor also exploited these vulnerabilities. The evolving regional dynamics in the Indo-Pacific are heightening the risk of crises, and it's likely that states will use cyber operations as a tool to challenge the sovereignty of others.[xliii] UK NCSC observed that Russia's February 2022 invasion of Ukraine was supported by vast cyber activity. In numerous cases, Russian cyber operations have been synchronized with their kinetic military activities. Initial signs of such cyber activities often manifested as DDoS (Distributed Denial of Service) attacks and the deployment of destructive wiper malware targeting various Ukrainian entities.[xliv] According to ACSC during the 2021–22 financial year, destructive malware used by Russia resulted in significant damage in Ukraine itself, also causing collateral damage to European networks and higher risk to networks worldwide.[xlv]

New Zealand NCSC reported that the most significant CVE disclosed in the 2021/2022 year was the Apache Log4j vulnerability. In December 2021, a significant vulnerability was identified in Apache Log4j, a widely used open-source logging library in many Java-based applications. This flaw exposed global networks to various cyber threats, including the potential for remote system access by malicious actors, data theft, unauthorized data export, and malware infections. The New Zealand NCSC issued an advisory to its clients, providing guidance on mitigating this vulnerability and detecting associated cyber threats. Leveraging their MFN (Managed Firewall Network) capability, the NCSC could swiftly distribute thousands of indicators of Log4j-related activities and proactively block them in almost real-time, thereby safeguarding organizations in Aotearoa New Zealand. In December 2021 alone, MFN partners successfully interrupted over 20,000 Log4j-related incidents on their customer networks.[xlvi]

According to Sophos 2023, many aspects of the threat landscape have evolved over the past year, however, one of the most notable developments is the ongoing evolution and expansion of the cybercriminal economy. That ecosystem has increasingly transformed into an industry in its own right, complete with a network of supporting services and highly professionalized, systematic approaches to its operations.[xlvii]

Access brokers, ransomware, information-stealing malware, malware delivery, and other elements of cybercrime operations have reduced the entry barriers for aspiring cybercriminals.[xlviii] Criminal marketplaces like Genesis enable entry-level cybercriminals to buy malware

and malware deployment services. Subsequently, these cybercriminals can then sell stolen credentials and other data in bulk.[xlix]

**Social engineering** is the third category of threats distinguished in analysed reports. According to ENISA, it comprised a 7,88 percent of incidents over the reporting period.[l] ENISA observes, that social engineering covers a wide range of tactics aimed at exploiting human errors or behaviours to gain access to information or services. It involves different manipulation strategies to deceive victims into making errors or handing over confidential or sensitive information. Users might be enticed to open documents, files, or emails, visit websites, or provide access to systems or services. While these lures and tricks might exploit technological aspects, their success primarily hinges on manipulating the human element. The primary attack vectors in this threat landscape include phishing, spear-phishing, whaling, smishing, vishing, watering hole attack, baiting, pretexting, quid pro quo, honeytraps and scareware. While commonly employed to secure initial access, social engineering methods can also be utilized in later stages of an incident or breach. Prominent examples include business email compromise (BEC), fraud, impersonation, counterfeiting, and, more recently, extortion.[li] According to Truesec 2023, social engineering is a significant factor in numerous cyber breaches. Phishing emails, which primarily use social engineering, deceive employees into inadvertently assisting criminals from within the organization.[lii]

CrowdStrike noted a rise in social engineering tactics involving direct human contact, like vishing, which have effectively distributed malware or bypassed multifactor authentication (MFA). This trend highlights the ongoing significance of personal interaction in the success of cybercrime activities.[liii] The growing prevalence of malware-free attacks and social engineering strategies aimed at gaining access or credentials underscores the inadequacy of traditional endpoint-only security solutions. The need for integrated identity protection, closely coordinated across endpoints, identity, and data, has become crucial. Implementing conditional, risk-based access policies is key to minimizing the burden and fatigue of multifactor authentication (MFA) for legitimate users.[liv] Truesec 2023 added that with organisations' increasing adoption of multifactor authentication (MFA), cybercriminals are turning to social engineering attacks to circumvent MFA protections. These social engineering tactics can range from straightforward brute force attacks, where the attacker persistently attempts to log in, hoping the targeted victim will inadvertently approve their access, to more complex schemes. In these elaborate setups, the attacker might impersonate an employee within the organization, contacting IT support to seek assistance in accessing the network, thus exploiting human vulnerability within the security chain. [lv]

According to CrowdStrike, since at least March 2022, SCATTERED SPIDER has been executing focused social engineering campaigns, predominantly targeting companies in the customer relationship management and business process outsourcing sectors. This adversary mainly employs phishing pages to harvest authentication details for systems like Okta, VPNs, or edge devices. Additionally, they manipulate users into divulging their one-time password MFA codes or exploit them by creating fatigue through repeated MFA notifications.[lvi] Once initial access is obtained, SCATTERED SPIDER employs a broad range of legitimate remote monitoring and management tools, along with utilities like PuTTY, to maintain persistent access.[lvii]

SCATTERED SPIDER utilizes its access to technology firms to target third-party companies, notably focusing on customers of the attacked businesses, with a significant emphasis on infiltrating cellular service providers. Although the full operational objectives of SCATTERED SPIDER aren't completely known, the adversary has been detected engaging in SIM swapping via access to these cellular services. This tactic of SIM swapping is presumed to facilitate subsequent compromises of third-party entities. [lviii]

According to Truesec 2023, effective cybersecurity should incorporate measures that reduce employee vulnerability to these social engineering attacks. However, the ultimate defence against such threats also heavily depends on human vigilance. The success of social engineering tactics can likely be attributed to insufficient training and awareness among personnel in recognizing and evading these types of attacks. Implementing MFA is crucial for securing your environment, yet the effectiveness of this protection hinges on your staff's correct response to prompts from MFA authenticators. This necessitates comprehensive training, as people are routinely overwhelmed with authentication requests, ranging from web cookies to login attempts. Maintaining constant alertness in these conditions can be challenging. Additionally, fostering a workplace culture where "there are no stupid questions" is vital. Such an environment encourages employees to freely approach the security team with any queries or doubts, further strengthening the organization's cybersecurity posture.[lix] Sophos 2023 observed that technology plays a vital role in detecting and preventing intrusions, but the true cornerstone in averting breaches lies with the security teams. For these teams, regular practice is key to perfection. It's important to foster an environment that consistently engages in tabletop exercises and red/blue team simulations to pinpoint and rectify vulnerabilities in cybersecurity strategies and responses. Moreover, it's not just the security teams that should be involved in these exercises — initiating user-awareness programs is crucial to counter the persistent threats of phishing and other forms of social engineering.[lx]

According to Truesec 2023, some cybercriminals are experimenting with even more sophisticated social engineering attacks. [lxi] The FBI recently alerted the public that an unidentified threat actor, posing as an IT engineer, applied for a remote role at a major IT company. In an elaborate scheme, the attacker used photos of the person they were impersonating to generate an AI-driven deepfake for the job interview conducted remotely. The goal was to secure employment in a remote position, thereby gaining access to the company's network. Truesec has also noted that cybercriminals are increasingly trying to procure software for AI programming to create deepfake videos. With the rapid advancements in AI chat technologies like "ChatGPT," there's a growing likelihood that these tools will be exploited to enhance social engineering tactics. This could lead to more convincing phishing emails and potentially enable partial automation of social engineering attacks in the future.[lxii]

**Threats against data** is another category of threats distinguished in analysed reports, comprising 20,09 percent of incidents over reporting period.[lxiii] Data breach is defined in the GDPR as *any breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed* (article 4.12 GDPR). ENISA has highlighted that, from a technical standpoint, threats targeting data can primarily be categorized as either a data breach or a data leak. While these

terms are often used interchangeably, they represent distinct concepts, mainly differing in their mode of occurrence. A data breach refers to a deliberate cyber-attack orchestrated by a cybercriminal with the aim of unauthorized access and dissemination of sensitive, confidential, or protected information. In essence, a data breach is a targeted and aggressive assault on a system or organization with the motive of data theft. On the other hand, a data leak is an incident (which could result from misconfigurations, vulnerabilities, or human mistakes) leading to the inadvertent loss or exposure of sensitive, confidential, or protected information. It's worth noting that intentional attacks sometimes fall under the term "data exposure".[lxiv]

According to UK NCSC, hacking of social media and email accounts, aimed at extorting money from victims for account access or to compromise data for committing or facilitating fraud, has seen a significant rise over the past year. In the period of 2021/22, there were a total of 8,023 reported instances of social media account hacking, marking a 23.5% increase compared to the previous year.[lxv] In 2022, CrowdStrike noted a 20% rise in the number of adversaries engaging in data theft and extortion campaigns, notably without the deployment of ransomware.[lxvi]

According to ACSC, Cybercriminals are increasingly focusing on employees' and customers' Personal Identifiable Information (PII), aiming to maximize the commercial and reputational damage caused by data breaches. In the most recent financial year, human resources organizations, especially those involved in payroll and recruitment, have become prime targets for ransomware attackers. These organizations are particularly vulnerable because they offer services across various sectors. In the fiscal year 2021–22, breaches of payroll service providers resulted in the access and exposure of data belonging to hundreds of thousands of Australian employees.[lxvii] Organizations providing social assistance, holding sensitive information about individuals, have been targeted by cybercriminals both in Australia and globally. A notable instance occurred in January 2022 when the Swiss-based International Committee of the Red Cross disclosed that a ransomware attack on its servers had compromised the personal data of over half a million individuals. This breach affected a wide range of people, including refugees and those internally displaced in conflict areas around the world.[lxviii]

Ransomware groups are diversifying their operations, as evidenced by the expanding use of leak sites. These sites are where cybercriminals publish information about their victims. The traditional model has been straightforward: if the targeted organizations pay the ransom, their data is kept off the leak site; if they refuse to pay, their data is published.[lxix]

**Threats against availability and integrity of data** is another significant category of threats. According to ENISA, it comprises 21,4 percent of DDoS over the reporting period.[lxx] DDoS attacks, which primarily target the availability of systems and data, remain a significant component in the cybersecurity threat landscape. These attacks hinder users from accessing necessary data, services, or resources by overwhelming or exhausting the service and its resources or overloading the network infrastructure's components.[lxxi]

**Disinformation and misinformation (or information manipulation)** comprised 4,81 percent of incidents over reporting period.[lxxii] According to ENISA, Foreign Information Manipulation and Interference (FIMI) refers to a pattern of behavior, often not illegal, that threatens or potentially negatively impacts values, procedures, and political processes. FIMI activities are characterized by their manipulative nature, conducted with intent and coordination. Both state and non-state actors, along with their proxies within and outside their territories, can engage in FIMI. This report examines the threat of FIMI, irrespective of its origin.[lxxiii]

As reported by UK UNSC, malicious cyber actors frequently use disinformation to create confusion and exploit divisions among target groups. In the context of the Russian invasion of Ukraine, Russian leadership propagated disinformation and misinformation globally about Ukraine and its allies to advance their preferred narrative. To counter this Russian disinformation, the unprecedented release of intelligence by the Five Eyes intelligence alliance has played a vital role. Although the UK NCSC has a limited role in addressing disinformation, it remains attentive to reports from security partners and the public regarding such disinformation campaigns.[lxxiv]

According to Sophos 2023, following the invasion of Ukraine by Russia, the Russian government was poised to strongly incentivize its domestic cybercriminal syndicates to sway global opinion in its favour, while undermining the international support garnered by the Ukrainian President. This led to a concerted effort by ransomware operators, malware distributors, and disinformation cells to mobilize in support of Russia's military actions. These groups activated their resources and capabilities to disseminate pro-Russian narratives and disrupt the digital solidarity with Ukraine, marking a significant moment where cyber operations and geopolitical strategies converged.[lxxv] Ukraine is currently facing a severe cyber threat environment, with less extensive but notable disturbances affecting the broader Western world. The risk of escalating conflict, misinformation, and further instability continues to be a significant concern. [lxxvi]

**A supply chain attack** is the last threat category distinguished by ENISA and other reports. According to ENISA, a supply chain attack targets the relationship between organisations and their suppliers. As stated in the ENISA Threat Landscape for Supply Chain Attacks, an attack is considered to have a supply chain component when it consists of a combination of at least two attacks.[lxxvii] An attack is defined as a supply chain attack when it involves compromising both the provider and their clients. The SolarWinds incident highlighted this attack vector and its far-reaching consequences, where malicious cyber actors strategically compromised a legitimate software update before the software provider's distribution. Different states attributed the activity to Russian state-sponsored actors in April 2021.[lxxviii] Threat actors persist in exploiting supply chains to infiltrate organizations, taking advantage of these interconnected systems' extensive reach and multitude of potential victims.[lxxix]

As reported by UK NCSC, global supply chain vulnerabilities remained evident as attackers infiltrated networks of target organizations through third-party vendors or suppliers. The exposure of the Log4J vulnerability underscored the difficulties posed by flaws in IT systems that can be leveraged to execute effective attacks.[lxxx]

The swiftly expanding and ever-more complex technology ecosystem presents greater opportunities for criminals and state actors to pursue their objectives. Supply chain attacks demonstrate how adversaries exploit the complexity of this ecosystem: if they can't directly breach an organization, they might exploit weak security in the organization's digital supply chain instead. In the past year, the danger to the global IT infrastructure from foreign states and cybercriminals has likely increased, with both groups enhancing their capabilities in targeting the IT sector. Foreign states often aim at entities to gather intelligence, whereas cybercriminals primarily engage in ransomware or data extortion attacks to generate profit.[lxxxi]

As reported by New Zealand NCSC, current organizations need to focus on securing their own networks and their entire supply chain. With the swift global adoption of IoT devices and connected systems, organizations rely on services that extend beyond their immediate oversight and control. Outsourcing technology services can enhance productivity and security. However, it also widens the potential attack surface, thus elevating the risk of exposure to cyber threats.[lxxxii] The interconnectedness of the online environment, together with the comprehensive nature of global supply chains and interoperability of technology, leaves networks worldwide increasingly exposed to a range of potential cyber-related impacts. A recent development in supply chain compromise involves the exploitation of software updates as a means of establishing a presence in customer systems.[lxxxiii] The New Zealand NCSC assessed that both state- and non-state-sponsored groups will likely continue to seek ways to exploit the digital transformation of organisations, and to infiltrate supply chains via weak access points.[lxxxiv]

According to ACSC, foresees the trend of cyber adversaries seeking to compromise multiple victims across various sectors through a single point of entry to persist. For instance, during 2021–22, Managed Service Providers (MSPs) were particularly targeted because they serve a wide range of clients, including government entities, commercial businesses, and not-for-profits of all sizes, making them appealing targets. Malicious actors progressively consider the supply chain a high-priority target and a means for widespread compromise.[lxxxv]

In addition, Truesec 2023 reported that Cybercriminals have identified that open-source code libraries can be exploited for supply chain attacks. They have targeted platforms such as GitHub and GitLab, creating forks of widely used code libraries that harbour malware. If these corrupted versions are downloaded, they can infect the user's system. Additionally, some malicious code libraries employ 'typosquatting' to mimic legitimate libraries, deceiving users into downloading compromised versions. There have been thousands of such malevolent code libraries found on GitHub, posing as reputable ones but containing malware. [lxxxvi]

Based on the conducted analysis, the following **new threats** could be distinguished from the analysed reports:

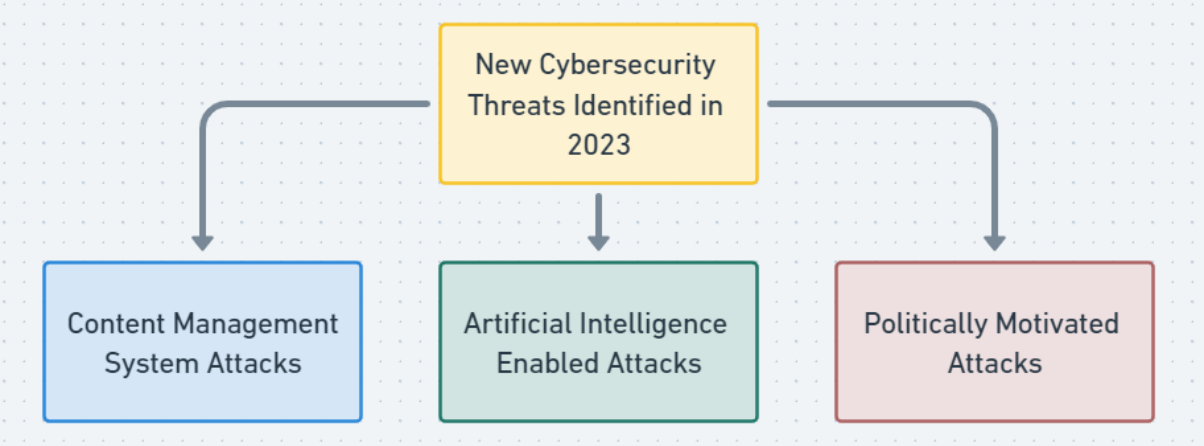


***Figure 4. New Cybersecurity Threats Identified in 2023***

**Content Management System (CMS) risk** is an attack on a Content Management System (CMS) software and refers to any unauthorized and malicious activity aimed at compromising the security of a CMS platform. CMS software is used to create, manage, and publish digital content on websites, and because it plays a central role in many websites, it is a common target for various types of cyberattacks. According to statistics available at that time, WordPress was estimated to be used by over 40% of all websites on the internet. The main attacks include: Brute Force attempts, Vulnerability Exploitation, SQL Injection, Cross-Site Scripting (XSS), DDoS attacks, Malware infections, Phishing, and File Inclusion attacks.[lxxxvii]

**AI (Artificial Intelligence) and generative AI-enabled** attacks refer to cyberattacks that leverage artificial intelligence and generative AI techniques to enhance their capabilities and effectiveness. These attacks use AI algorithms and machine learning models to automate and optimize various aspects of the attack process. Attackers use AI to create evolving malware, employ AI algorithms for convincing phishing emails, generate deepfake content for impersonation or disinformation, conduct automated social engineering based on analyzed social media data, accelerate password cracking with AI, analyze network traffic using AI for vulnerabilities, and spread disinformation through AI-generated content.[lxxxviii]

Truesec 2023 has also noted that cybercriminals are increasingly trying to procure software for AI programming to create deepfake videos. With the rapid advancements in AI chat technologies like “ChatGPT,” there’s a growing likelihood that these tools will be exploited to enhance social engineering tactics. This could lead to more convincing phishing emails and potentially enable partial automation of social engineering attacks in the future.[lxxxix]

**Politically motivated attacks or hacktivism**: are malicious actions carried out in the digital realm with the primary goal of advancing a political agenda or ideology. These attacks are typically driven by ideological, social, or geopolitical motivations, and they can target governments, political organizations, institutions, corporations, or individuals who are perceived as opposing or representing a threat to the attacker's beliefs or interests.[xc] According to CrowdStrike 2023, in 2022, hacktivists embraced the climate of misinformation, seizing upon significant geopolitical changes to fuel national unrest and propagate particular ideologies.

Although their actions were primarily focused on targets within the Russo-Ukrainian area, there was a notable increase in collateral activities where entities in neighbouring regions, Europe, and the United States were targeted. This spillover of activities intensified from the second half of 2022 and continued into 2023, reflecting hacktivist operations' expanding scope and impact.[xci]

According to New Zealand NCSC, Cyber actors expressing support for Russia, as well as those siding with Ukraine, are actively participating in cyber operations linked to the conflict. On the pro-Ukraine side, cyber operations have been conducted by the 'hacktivist' group Anonymous, as well as by individual cyber volunteers enlisting with the IT Army of Ukraine. Pro-Russia cyber activities in relation to the invasion have involved groups such as Killnet, Ghostwriter, and Conti, each engaging in various cyber operations.[xcii] The proliferation of cyber vigilantes contributes to the risk of accidental escalation. This has presented challenges on the development of international cyber norms and raising questions about what constitutes a proportionate and acceptable response to threats posed by hostile states.[xciii]

To sum up, the analysis of the last year's sectoral surveys and national threat trends reports reveals a persistent and evolving landscape of cybersecurity threats, with ransomware, malware, and social engineering tactics remaining at the forefront. Despite different patterns and techniques employed by cybercriminals, the consistent rise in ransomware incidents, particularly within critical infrastructure and the adoption of new extortion methods, underlines the ongoing and complex challenges facing cybersecurity professionals. The increased sophistication of ransomware as a service (RaaS), politically motivated attacks, and the leveraging of AI technologies for cyberattacks highlight the need for a dynamic and robust cybersecurity strategy. As threats diversify and tactics become more nuanced, it is crucial for organizations to enhance their defensive measures, improve incident response strategies, and invest in continuous skill development to mitigate the risks of these emerging threats.

# 5. CYBERSECURITY SKILLS REQUIRED TO ADDRESS IDENTIFIED THREATS

The purpose of this chapter is to map the main identified cybersecurity threats with the skills required to address the respective threats and link it with the 12 ECSF role profiles.

## 5.1. Skills and threats mapping methodology

The following methodology has been considered for mapping the identified threats to cybersecurity skills, according to three main axes:

- **Identification of threats and skills.** To perform this mapping, we relied on the updated list of cybersecurity threats, which was based on a comprehensive review of all threats documented in the year 2022, carefully evaluating their ongoing relevance to the current year, ensuring that they maintain their significance, and on a rigorous examination of most recent 2023 reports, meticulously sifting through their contents. It is also pertinent to emphasize that the requisite job profiles and the associated skills essential for this endeavour have already been thoughtfully detailed and provided within the scope of WP3 through the latest version of the cybersecurity skills framework.

- **Association of skills with threats.** To effectively address each identified threat, our approach involves an assessment of which precise skills are most pertinent for mitigating or countering these specific identified threats. For instance, threat analysis entails gaining deep insights into the threat's distinctive characteristics, tactics and techniques. We also delve into evaluating its potential impact, the vectors of attack and the vulnerabilities it exploits. Our methodology is firmly rooted in established best practices and practical expertise, ensuring a robust and well-informed strategy for threat mitigation and response.

- **Assignment of weights for the mapping**. To make a systematic assessment, we have complemented the mapping with a method of assigning numerical weightings for each skill coming from the ECSF role profiles, with the purpose of quantifying its significance in addressing each specific threat. These weightings are designed to accurately reflect the skill efficiency in mitigating the given cybersecurity threat. For this, we have utilized a scale that ranges from 1 to 5, with the weight of 5 signifying the utmost importance and effectiveness in countering the considered cybersecurity threat.

## 5.2. Mapping results

In this section, we detail the different tables that map the cyber threats across the three considered categories: Operational Technology (OT) Threats, Information Technology (IT)





REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Threats, and shared Information Technology Threats, to the skills related to 12 ECSF role profiles. For clarity, we provide two tables for each threat categories, the first table corresponding the first six role profiles, and the second table corresponding to the second six role profiles from the ENISA cybersecurity skills framework. From these tables, we then elaborate on the skills that are the most relevant in addressing the identified threats and the job profiles associated with these skills. We also analyse the coverage of threats by skills for each of the three main threat categories and discuss some refinement of skills to properly address such threats.

### 5.2.1. Operational Technology (OT) Threats

Table 6 serves as a detailed reference for understanding the link between Operational Technology (OT) threats and the first 6 ECSF role profiles equipped to address them. Each cell within the table contains a curated list of skills associated with a specific job profile, highlighting the expertise required to mitigate Operational Technology (OT) cybersecurity threats effectively.

The mapping of skills with respect to OT threats shows the importance of several key skills from the ENISA cybersecurity skills framework. In particular, effective communication, coordination, and cooperation with internal and external stakeholders is crucial for addressing these cybersecurity threats. Ensuring seamless information sharing, and coordinating responses are essential to properly counter threats, such as those related to the cybersecurity workforce gap, the outsourcing of third parties for ICS architecture management, the remote access to the corporate network, the reliance on external servers for critical infrastructure, and the integration of IT and OT networks. Recognizing and categorizing types of vulnerabilities and their associated attacks are also required to enable proactive measures to secure such systems. Utilizing cyber threat intelligence (CTI) platforms and tools enables also staying well-informed about emerging threats and attack patterns. In addition, conducting ethical hacking, identifying, and solving cybersecurity-related issues, as well as assessing cybersecurity vulnerabilities contribute to address several others, such those related to the vulnerabilities of ICS components, to the use of outdated and obscure components and to content management systems. These skills empower organizations to anticipate Operational Technology (OT) threats and manage the relevant risks in a more efficient manner.

The analysis of the first mapping reveals that all the Operational Technology (OT) threats are covered by at least two skills from the ENISA cybersecurity skills framework. In addition, some skills could be further refined to consider the threats' specificities. In particular, the threats related to the vulnerabilities of ICS components might be covered by more specific skills about the security of ICS systems, such as those linked to SCADA systems, PLCs and more generally to network protocols used in OT environments, by contributing to a more precise response to such threats. In the same manner, cybersecurity threats related to the outsourcing of third parties to manage and maintain the ICS architecture could be further covered by more refined skills on OT security frameworks and standards, as well as on specific industrial processes and technologies.

Overall, this mapping with respect to Operational Technology (OT) threats highlights more specifically, amongst the twelves job profiles from the ENISA skills framework, the following

ones: the penetration tester, the cyber threat intelligence specialist, the cybersecurity educator, the cybersecurity architect, and the cyber incident responder.

***Table 1. The skills and knowledge required to effectively mitigate Operational Technology cybersecurity threats for the first set of the ECSF role profiles***

| Identified threats | CHIEF INFORMATION SECURITY OFFICER (CISO) | CYBER INCIDENT RESPONDER | CYBER LEGAL, POLICY & COMPLIANCE OFFICER | CYBER SECURITY AUDITOR | CYBER THREAT INTELLIGENCE SPECIALIST | CYBERSECURITY ARCHITECT |
|---|---|---|---|---|---|---|
| **OPERATIONAL TECHNOLOGY THREATS** | | | | | | |
| **Cybersecurity workforce gap** | Influence an organisation's cybersecurity culture (weight: 2.5)<br>Motivate and encourage people (weight: 4)<br>Guide, direct and motivate others. (weight: 4) | - | Understand, practice and adhere to ethical requirements and standards (weight: 4)<br>Educate, monitor and assess the awareness of organization members and external parties on cybersecurity and privacy issues as needed. (weight: 5) | Communicate, coordinate and cooperate with internal and external stakeholders (weight: 4) | Communicate, coordinate and cooperate with internal and external stakeholders (weight: 4) | Define, present and promote an information security policy for approval by the senior management of the organization (weight: 3) |
| **Vulnerabilities of ICS components** | - | Recognize and categorize types of vulnerabilities and associated attacks (weight: 3) | - | - | Use and apply CTI platforms and tools (weight: 4)<br>Automate threat intelligence management procedures (weight: 3) | Coordinate the integration of security solutions (weight: 3.5)<br>Monitor progress of issues throughout lifecycle and communicate effectively (weight: 3)<br>Contribute to the development of ICT strategy and policy, including ICT security and quality (weight: 3) |

| Identified threats | CHIEF INFORMATION SECURITY OFFICER (CISO) | CYBER INCIDENT RESPONDER | CYBER LEGAL, POLICY & COMPLIANCE OFFICER | CYBER SECURITY AUDITOR | CYBER THREAT INTELLIGENCE SPECIALIST | CYBERSECURITY ARCHITECT |
|---|---|---|---|---|---|---|
| **OPERATIONAL TECHNOLOGY THREATS** | | | | | | |
| **Content Management System (CMS) software** | Implement cybersecurity recommendations and best practices (weight: 4) | Secure network communications (weight: 4)<br><br>Manage and analyse log files (weight: 4), Collect, analyse and correlate cyber threat information originating from multiple sources (weight: 3) | - | - | Coordinate the integration of security solutions (weight: 3) | - |
| **Unpatched components** | - | - | - | - | - | Plan and implement application and data provisioning (weight: 4)<br>Monitor progress of issues throughout lifecycle and communicate effectively (weight: 3) |
| **Utilizing of outdated and obscure components** | - | - | - | Assess risk factors (weight: 4) | - | Contribute to the development of ICT strategy and policy, including ICT security and quality (weight: 3) |
| **Outsourcing of the third parties to manage and maintain the ICS architecture** | - | - | - | Communicate, coordinate and cooperate with internal and external stakeholders (weight: 4) | Communicate, coordinate and cooperate with internal and external stakeholders (weight: 4) | - |

| Identified threats | CHIEF INFORMATION SECURITY OFFICER (CISO) | CYBER INCIDENT RESPONDER | CYBER LEGAL, POLICY & COMPLIANCE OFFICER | CYBER SECURITY AUDITOR | CYBER THREAT INTELLIGENCE SPECIALIST | CYBERSECURITY ARCHITECT |
|---|---|---|---|---|---|---|
| **OPERATIONAL TECHNOLOGY THREATS** | | | | | | |
| **Remote access to the corporate network** | - | - | Enforce and advocate organisation's data privacy and protection program (weight: 4) Explain and communicate data protection and privacy topics to stakeholders and users (weight: 4) | - | Use and apply CTI platforms and tools (weight: 3) | Contribute to the development of ICT strategy and policy, including ICT security and quality (weight: 3) |
| **Utilizing external servers for critical infrastructure architecture** | - | Work on operating systems, servers, clouds and relevant infrastructures (weight: 4) | - | Communicate, coordinate and cooperate with internal and external stakeholders (weight: 2.5) | Use and apply CTI platforms and tools (weight: 4) Communicate, coordinate and cooperate with internal and external stakeholders (weight: 2.5) | - |
| **Integration of IT and OT networks** | - | Work on operating systems, servers, clouds and relevant infrastructures (weight: 4) | - | - | Use and apply CTI platforms and tools (weight: 3) | Guide and communicate with implementers and IT/OT personnel (weight: 4) |

***Table 2. The skills and knowledge required to effectively mitigate Operational Technology cybersecurity threats for the second set of the ECSF role profiles***

| Identified threats | CYBERSECURITY EDUCATOR | CYBERSECURITY IMPLEMENTER | CYBERSECURITY RESEARCHER | CYBERSECURITY RISK MANAGER | DIGITAL FORENSICS INVESTIGATOR | PENETRATION TESTER |
|---|---|---|---|---|---|---|
| **OPERATIONAL TECHNOLOGY THREATS** | | | | | | |
| **Cybersecurity workforce gap** | Utilise existing cybersecurity-related training resources (weight: 3)<br><br>Advise on appropriate solutions in the field of skills certification schemes, taking into consideration the needs of the interested parties (weight: 4)<br><br>Convey complex information, concepts, or ideas effectively through verbal, written, and/or visual means and to different levels of audience (weight: 4)<br><br>Gauge learner understanding and knowledge level and, provide effective feedback to students for improving learning (weight: 3) | Communicate, present and report to relevant stakeholders (weight: 4) | Communicate, present and report to relevant stakeholders (weight: 4)<br>Generate new ideas and transfer theory into practice (weight: 3)<br>Communicate, present and report (weight: 3.5) | Communicate, present and report to relevant stakeholders (weight: 4) | - | Communicate, present and report to relevant stakeholders (weight: 4)<br>Explain and communicate technical cybersecurity topics appropriately to a variety of stakeholders. (weight: 4) |
| **Vulnerabilities of ICS components** | Monitor evolving security and privacy | - | - | - | Recognize and categorize types | Conduct ethical hacking (weight: 4) |

| Identified threats | CYBERSECURITY EDUCATOR | CYBERSECURITY IMPLEMENTER | CYBERSECURITY RESEARCHER | CYBERSECURITY RISK MANAGER | DIGITAL FORENSICS INVESTIGATOR | PENETRATION TESTER |
|---|---|---|---|---|---|---|
| **OPERATIONAL TECHNOLOGY THREATS** | | | | | | |
| | infrastructures, technologies and methods (weight: 3) | | | | of vulnerabilities and associated attacks (weight: 2.5) | Identify and solve cybersecurity-related issues (weight: 4)<br>Assess cybersecurity vulnerabilities (weight: 4) |
| **Content Management System (CMS) software** | Monitor evolving security and privacy infrastructures, technologies and methods (weight: 3) | - | - | - | - | Conduct ethical hacking (weight: 4)<br>Identify and solve cybersecurity-related issues (weight: 4) |
| **Unpatched components** | - | Develop code, scripts and programmes (weight: 3) | - | Build a cybersecurity risk-aware environment (weight: 2.5) | - | Conduct ethical hacking (weight: 4)<br>Identify and solve cybersecurity-related issues (weight: 4)<br>Develop codes, scripts and programmes (weight: 3) |
| **Utilizing of outdated and obscure components** | Monitor evolving security and privacy infrastructures, technologies and methods (weight: 3) | Develop code, scripts and programmes (weight: 3) | - | - | - | Conduct ethical hacking (weight: 4)<br>Identify and solve cybersecurity-related issues (weight: 4) |
| **Outsourcing of the third parties to manage and maintain the ICS architecture** | - | - | - | - | - | - |
| **Remote access to the corporate network** | Apply network protection components and security controls (weight: 4.5) | - | Conduct network configuration and setup (weight: 4) | - | - | Conduct ethical hacking (weight: 4)<br>Identify and solve cybersecurity-related issues (weight: 4) |

| Identified threats | CYBERSECURITY EDUCATOR | CYBERSECURITY IMPLEMENTER | CYBERSECURITY RESEARCHER | CYBERSECURITY RISK MANAGER | DIGITAL FORENSICS INVESTIGATOR | PENETRATION TESTER |
|---|---|---|---|---|---|---|
| **OPERATIONAL TECHNOLOGY THREATS** | | | | | | |
| **Utilizing external servers for critical infrastructure architecture** | - | - | - | Build a cybersecurity risk-aware environment (weight: 3) | - | - |
| **Integration of IT and OT networks** | - | - | Conduct network configuration and setup (weight: 4) | - | - | - |

## 5.2.2. Information Technology (IT) Threats

Table 8 and Table 9 provide a comprehensive mapping between Information Technology (IT) threats and first and the second 6 ECSF role profiles. Each cell of the table provides a list of skills associated with a particular job profile that can be harnessed to counter the specific IT security threat outlined.

The mapping of skills with respect to Information Technology (IT) threats also provides interesting elements regarding the key skills from the ENISA cybersecurity skills framework for addressing such threats. In particular, securing network communications is of major importance to prevent multiple cybersecurity threats, including compromising of communication equipment, network eavesdropping, traffic analysis, broken authentication, and man-in-the-middle attacks. Applying network protection components and security controls contribute complementarily to such prevention against DDoS attacks, POS intrusions, DNS cache poisoning, and DNS spoofing. Conducting ethical hacking, as already shown with the Operational Technology (OT) threats, enables identifying vulnerabilities at an early stage to prevent their exploitation through cybersecurity attacks, and enables addressing several threats, such as those regarding injection flaws, cross-site scripting, insecure deserialization, and more generally web application attacks and advanced persistent threats (APT). Using specific tools, techniques, and methods in relation to digital forensics helps in investing the root cause of an attack, and in better quantifying its impact, in link with threats such as vulnerabilities affecting mobile applications or ransomware campaigns. Skills regarding security and privacy infrastructures, technologies, and methods also permit to address critical threats, such as privacy infringements and identity theft.

The analysis of this second mapping shows that around 75% of the Information Technology (IT) threats are covered by at least two skills from the ENISA cybersecurity skill framework. In addition, the refinement of some skills could contribute to better address some of the identified threats. More specifically, the threat related to large-scale attacks on IoT (medical devices) could benefit from skills more specific to medical device protection and regulations. Secure firmware development, data transmission, and lifecycle management, network segmentation, and real-time monitoring can further strengthen medical IoT devices' security. Also, the threats regarding social engineering are increased by the advances in the area of generative artificial intelligence. This requires further understanding of AI-driven social engineering tactics, and better exploitation of methods and techniques for efficiently detecting and countering AI-enhanced attacks, such advanced phishing and deepfake contents. Also, the lack of protective monitoring could take benefits from the efforts done in the area of software-defined networking, with the new capabilities offered by these networking environments in terms of programmability and flexibility.

Overall, the mapping with respect to Information Technology (IT) threats highlights more specifically, amongst the 12 ECSF role profiles from the ENISA skills framework, the following ones: the penetration tester, the cyber incident responder, the cybersecurity educator, the digital forensics investigator, and the chief information security officer.

***Table 3. The skills and knowledge required to effectively mitigate Information technology cybersecurity threats for the first set of the ECSF role profiles***

| Identified threats | CHIEF INFORMATION SECURITY OFFICER (CISO) | CYBER INCIDENT RESPONDER | CYBER LEGAL, POLICY & COMPLIANCE OFFICER | CYBER SECURITY AUDITOR | CYBER THREAT INTELLIGENCE SPECIALIST | CYBERSECURITY ARCHITECT |
|---|---|---|---|---|---|---|
| **INFORMATION TECHNOLOGY THREATS** | | | | | | |
| **AI (Artificial Intelligence) and generative AI-enabled** | Apply security design principles, e.g. least privilege (weight: 3) | - | - | - | Collect, analyse and correlate cyber threat information originating from multiple sources (weight: 3) | - |
| **Malware exploits** | - | Protect a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters) (weight: 4) | - | - | - | Monitor progress of issues throughout lifecycle and communicate effectively (weight: 3) |
| **Ransomware** | - | - | - | - | - | - |
| **Privacy Infringement** | Implement cybersecurity recommendations and best practices (weight: 3) | - | Enforce and advocate organisation's data privacy and protection program (weight: 4)<br>Explain and communicate data protection and privacy topics to stakeholders and users (weight: 4) | - | - | - |
| **Identity theft** | Implement cybersecurity recommendations and | - | Enforce and advocate organisation's data privacy and protection program (weight: 4) | - | - | - |

| Identified threats | CHIEF INFORMATION SECURITY OFFICER (CISO) | CYBER INCIDENT RESPONDER | CYBER LEGAL, POLICY & COMPLIANCE OFFICER | CYBER SECURITY AUDITOR | CYBER THREAT INTELLIGENCE SPECIALIST | CYBERSECURITY ARCHITECT |
|---|---|---|---|---|---|---|
| **INFORMATION TECHNOLOGY THREATS** | | | | | | |
| | best practices (weight: 3) | | | | | |
| **Compromising of communication equipment** | - | Secure network communications (weight: 3) | - | - | - | - |
| **Web applications attack** | - | - | - | - | - | Plan and implement application and data provisioning (weight: 3) |
| **Vulnerabilities in Mobile Applications and payment interfaces** | Communicate and promote the organisation's risk analysis outcomes and risk management processes (weight: 3) | Secure network communications (weight: 3) | - | - | - | - |
| **Data Confidentiality, Integrity and Availability** | - | Secure network communications (weight: 3) | Enforce and advocate organisation’s data privacy and protection program (weight: 4.5) | Follow and practice auditing frameworks, standards and methodologies (weight: 4) | Collect, analyse and correlate cyber threat information originating from multiple sources (weight: 3) | Dealing with problems (weight: 3)<br>Contribute to the development of ICT strategy and policy, including ICT security and quality (weight: 3) |
| **Eavesdropping and traffic analysis** | - | Secure network communications (weight: 4) | - | - | - | - |
| **DDoS** | - | - | - | - | - | - |
| **Social Engineering** | Implement cybersecurity | - | - | - | - | - |

| Identified threats | CHIEF INFORMATION SECURITY OFFICER (CISO) | CYBER INCIDENT RESPONDER | CYBER LEGAL, POLICY & COMPLIANCE OFFICER | CYBER SECURITY AUDITOR | CYBER THREAT INTELLIGENCE SPECIALIST | CYBERSECURITY ARCHITECT |
|---|---|---|---|---|---|---|
| **INFORMATION TECHNOLOGY THREATS** | | | | | | |
| | recommendations and best practices (weight: 3) | | | | | |
| **POS intrusions** | Apply security design principles, e.g. least privilege (weight: 3) | - | - | - | - | - |
| **Miscellaneous errors** | - | - | - | - | - | - |
| **Lack of protective monitoring** | - | Collect, analyse and correlate cyber threat information originating from multiple sources (weight: 3.5) | - | - | - | Contribute to the development of ICT strategy and policy, including ICT security and quality (weight: 2.5) |
| **Vulnerabilities in automated machines (ATMs, cashier machines, POS intrusions)** | Apply security design principles, e.g. least privilege (weight: 4) | - | - | - | Collect, analyse and correlate cyber threat information originating from multiple sources (weight: 3) | - |
| **Large-scale attacks on IoT (medical devices)** | Apply security design principles, e.g. least privilege (weight: 2.5) | - | - | - | - | - |
| **Advanced Persistent Threats (APT)** | - | Recognize and categorize types of vulnerabilities | | - | - | Dealing with problems (weight: 2.5) |

| Identified threats | CHIEF INFORMATION SECURITY OFFICER (CISO) | CYBER INCIDENT RESPONDER | CYBER LEGAL, POLICY & COMPLIANCE OFFICER | CYBER SECURITY AUDITOR | CYBER THREAT INTELLIGENCE SPECIALIST | CYBERSECURITY ARCHITECT |
|---|---|---|---|---|---|---|
| **INFORMATION TECHNOLOGY THREATS** | | | | | | |
| | | and associated attacks (weight: 3) | | | | |
| **Intellectual property theft** | Communicate and promote the organisation's risk analysis outcomes and risk management processes (weight: 3) | - | Lead the development of appropriate cybersecurity and privacy policies and procedures that complement the business needs and legal requirements; further ensure its acceptance, comprehension and implementation and communicate it between the involved parties (weight: 4)<br>Perform (Implement) and Monitor audits against cybersecurity-related applicable laws, regulations and standards, collect needed evidence and document audit information and results, in alignment to the relevant audit plan(s). (weight: 3) | - | - | - |
| **Denial of Service (Dos)** | - | - | - | - | - | Conduct performance and resilience testing (weight: 4)<br>Contribute to the development of ICT strategy and policy, including ICT security and quality (weight: 3) |

| Identified threats | CHIEF INFORMATION SECURITY OFFICER (CISO) | CYBER INCIDENT RESPONDER | CYBER LEGAL, POLICY & COMPLIANCE OFFICER | CYBER SECURITY AUDITOR | CYBER THREAT INTELLIGENCE SPECIALIST | CYBERSECURITY ARCHITECT |
|---|---|---|---|---|---|---|
| **INFORMATION TECHNOLOGY THREATS** | | | | | | |
| **DNS Cache Poisoning** | - | - | - | - | - | - |
| **DNS Spoofing** | - | - | - | - | - | - |
| **Cybersquatting** | - | - | - | - | - | - |
| **Typosquatting** | - | - | - | - | - | - |
| **Adapting to risks from advances in employee computing technologies (e.g., increased prevalence of sensors, AI, etc.)** | - | - | Lead the development of appropriate cybersecurity and privacy policies and procedures that complement the business needs and legal requirements; further ensure its acceptance, comprehension and implementation and communicate it between the involved parties (weight: 4) | Apply auditing tools and techniques (weight: 3) | - | - |
| **Injection flaws** | - | - | - | - | - | - |
| **Broken authentication** | - | Secure network communications (weight: 3.5) | - | - | - | Plan and implement application and data provisioning (weight: 2.5) |
| **Broken access control** | Apply security design principles, e.g. least privilege (weight: 2.5) | Secure network communications (weight: 4) | - | - | - | - |
| **Cross-site scripting (XSS)** | - | - | - | - | - | - |
| **Man-in-the-middle attacks** | - | Secure network communications (weight: 4) | - | - | - | - |

| Identified threats | CHIEF INFORMATION SECURITY OFFICER (CISO) | CYBER INCIDENT RESPONDER | CYBER LEGAL, POLICY & COMPLIANCE OFFICER | CYBER SECURITY AUDITOR | CYBER THREAT INTELLIGENCE SPECIALIST | CYBERSECURITY ARCHITECT |
|---|---|---|---|---|---|---|
| **INFORMATION TECHNOLOGY THREATS** | | | | | | |
| **XML external entities (XXE)** | - | - | - | - | - | - |
| **Cryptojacking** | - | - | - | - | - | - |
| **Watering hole** | - | - | - | - | - | - |
| **Living off the land (LOTL)** | - | - | - | - | - | - |
| **Insecure deserialization** | - | - | - | - | Collect, analyse and correlate cyber threat information originating from multiple sources (weight: 3.5) | - |

***Table 4. The skills and knowledge required to effectively mitigate Information technology cybersecurity threats for the second set of the ECSF role profiles***

| Identified threats | CYBERSECURITY EDUCATOR | CYBERSECURITY IMPLEMENTER | CYBERSECURITY RESEARCHER | CYBERSECURITY RISK MANAGER | DIGITAL FORENSICS INVESTIGATOR | PENETRATION TESTER |
|---|---|---|---|---|---|---|
| **INFORMATION TECHNOLOGY THREATS** | | | | | | |
| **AI and generative AI-enabled** | - | - | - | | - | - |
| **Malware exploits** | - | - | - | - | - | Conduct ethical hacking (weight: 4)<br>Identify and solve cybersecurity-related issues (weight: 3.5) |
| **Ransomware** | - | - | - | - | Use specific tools, techniques and methods in relation to digital forensics (extracting, reversing and understanding code and traces, logs, malware analysis, protocols, operating systems, etc) (weight: 3) | - |
| **Privacy Infringement** | Monitor evolving security and privacy infrastructures, technologies and methods (weight: 4) | - | Decompose and analyse systems to develop security and privacy requirements (weight: 3) | Enable business assets owners, executives and other stakeholders to make risk informed decisions to manage and mitigate risks (weight: 3.5) | Use specific tools, techniques and methods in relation to digital forensics (extracting, reversing and understanding code and traces, logs, malware analysis, protocols, operating systems, etc) (weight: 3) | - |
| **Identity theft** | Monitor evolving security and privacy infrastructures, technologies | - | Decompose and analyse systems to develop security and | Enable business assets owners, executives and other stakeholders to | - | - |

| Identified threats | CYBERSECURITY EDUCATOR | CYBERSECURITY IMPLEMENTER | CYBERSECURITY RESEARCHER | CYBERSECURITY RISK MANAGER | DIGITAL FORENSICS INVESTIGATOR | PENETRATION TESTER |
|---|---|---|---|---|---|---|
| **INFORMATION TECHNOLOGY THREATS** | | | | | | |
| | and methods (weight: 4) | | privacy requirements (weight: 3) | make risk informed decisions to manage and mitigate risks (weight: 3.5) | | |
| **Compromising of communication equipment** | - | - | - | - | Use specific tools, techniques and methods in relation to digital forensics (extracting, reversing and understanding code and traces, logs, malware analysis, protocols, operating systems, etc) (weight: 4) | Conduct ethical hacking (weight: 4)<br>Identify and solve cybersecurity-related issues (weight: 4) |
| **Web applications attack** | - | - | - | - | Use specific tools, techniques and methods in relation to digital forensics (extracting, reversing and understanding code and traces, logs, malware analysis, protocols, operating systems, etc) (weight: 4) | Conduct ethical hacking (weight: 4)<br>Identify and solve cybersecurity-related issues (weight: 4) |
| **Vulnerabilities in Mobile Applications and payment interfaces** | - | - | - | - | Use specific tools, techniques and methods in relation to digital forensics (extracting, reversing and understanding code and traces, logs, malware analysis, protocols, operating systems, etc) (weight:3) | Conduct ethical hacking (weight:3)<br>Identify and solve cybersecurity-related issues (weight: 3)<br>Assess cybersecurity vulnerabilities (weight: 4) |
| **Data Confidentiality, Integrity and Availability** | Monitor evolving security and privacy | - | Decompose and analyse systems to develop security and | - | - | - |

| Identified threats | CYBERSECURITY EDUCATOR | CYBERSECURITY IMPLEMENTER | CYBERSECURITY RESEARCHER | CYBERSECURITY RISK MANAGER | DIGITAL FORENSICS INVESTIGATOR | PENETRATION TESTER |
|---|---|---|---|---|---|---|
| **INFORMATION TECHNOLOGY THREATS** | | | | | | |
| | infrastructures, technologies and methods (weight: 4) | | privacy requirements and identify effective solution (weight: 3) | | | |
| **Eavesdropping and traffic analysis** | - | - | - | - | - | Develop codes, scripts and programmes (weight: 2) |
| **DDoS** | Apply network protection components and security controls (weight: 4) | - | - | - | - | - |
| **Social Engineering** | Apply network protection components and security controls (weight: 2.5) | - | - | - | - | Perform social engineering (weight: 4) |
| **POS intrusions** | Apply network protection components and security controls (weight: 3) | - | - | - | Work ethically and independently; not influenced and biased by internal or external actors (weight: 4) | Conduct ethical hacking (weight: 4)<br>Identify and solve cybersecurity-related issues (weight: 4) |
| **Miscellaneous errors** | - | - | Identify effective solutions (weight: 3) | - | - | - |
| **Lack of protective monitoring** | - | - | - | - | - | - |
| **Vulnerabilities in automated machines (ATMs, cashier machines, POS intrusions)** | - | - | - | - | - | - |

| Identified threats | CYBERSECURITY EDUCATOR | CYBERSECURITY IMPLEMENTER | CYBERSECURITY RESEARCHER | CYBERSECURITY RISK MANAGER | DIGITAL FORENSICS INVESTIGATOR | PENETRATION TESTER |
|---|---|---|---|---|---|---|
| **INFORMATION TECHNOLOGY THREATS** | | | | | | |
| **Large-scale attacks on IoT (medical devices)** | - | - | - | - | - | - |
| **Advanced Persistent Threats (APT)** | - | - | - | - | - | - |
| **Intellectual property theft** | Monitor evolving security and privacy infrastructures, technologies and methods (weight: 3) | - | Decompose and analyse systems to develop security and privacy requirements (weight: 4) | - | - | - |
| **Denial of Service (Dos)** | Apply network protection components and security controls (weight: 3) | Conduct network configuration and setup (weight: 3) | - | - | Use specific tools, techniques and methods in relation to digital forensics (extracting, reversing and understanding code and traces, logs, malware analysis, protocols, operating systems, etc) (weight: 2.5) | Conduct ethical hacking (weight: 3)<br>Identify and solve cybersecurity-related issues (weight: 4) |
| **DNS Cache Poisoning** | Apply network protection components and security controls (weight: 3) | Conduct network configuration and setup (weight: 3) | - | - | Use specific tools, techniques and methods in relation to digital forensics (extracting, reversing and understanding code and traces, logs, malware analysis, protocols, operating systems, etc) (weight: 3) | Conduct ethical hacking (weight: 4)<br>Identify and solve cybersecurity-related issues (weight: 3.5) |
| **DNS Spoofing** | Apply network protection components and security controls (weight: 3) | - | - | - | Use specific tools, techniques and methods in relation to digital forensics (extracting, reversing and understanding code and | Conduct ethical hacking (weight: 3)<br>Identify and solve cybersecurity-related issues (weight: 4) |

| Identified threats | CYBERSECURITY EDUCATOR | CYBERSECURITY IMPLEMENTER | CYBERSECURITY RESEARCHER | CYBERSECURITY RISK MANAGER | DIGITAL FORENSICS INVESTIGATOR | PENETRATION TESTER |
|---|---|---|---|---|---|---|
| **INFORMATION TECHNOLOGY THREATS** | | | | | | |
| | | | | | traces, logs, malware analysis, protocols, operating systems, etc) (weight: 2.5) | |
| **Cybersquatting** | - | - | - | - | - | Conduct ethical hacking (weight: 3)<br>Identify and solve cybersecurity-related issues (weight: 4) |
| **Typosquatting** | - | - | - | - | - | Conduct ethical hacking (weight: 3)<br>Identify and solve cybersecurity-related issues (weight: 4) |
| **Adapting to risks from advances in employee computing technologies** | - | - | - | Use monitoring tools to measure and evaluate the effectiveness of implemented cybersecurity controls and the achieved security levels. (weight: 3.5) | - | Conduct ethical hacking (weight: 3)<br>Identify and solve cybersecurity-related issues (weight: 4) |
| **Injection flaws** | - | - | - | - | - | Conduct ethical hacking (weight: 3)<br>Identify and solve cybersecurity-related issues (weight: 4) |
| **Broken authentication** | - | - | - | - | - | Conduct ethical hacking (weight: 3)<br>Identify and solve |

| Identified threats | CYBERSECURITY EDUCATOR | CYBERSECURITY IMPLEMENTER | CYBERSECURITY RESEARCHER | CYBERSECURITY RISK MANAGER | DIGITAL FORENSICS INVESTIGATOR | PENETRATION TESTER |
|---|---|---|---|---|---|---|
| **INFORMATION TECHNOLOGY THREATS** | | | | | | |
| | | | | | | cybersecurity-related issues (weight: 4) |
| **Broken access control** | - | Conduct network configuration and setup (weight: 3) | - | - | - | Conduct ethical hacking (weight: 4)<br>Identify and solve cybersecurity-related issues (weight: 4) |
| **Cross-site scripting (XSS)** | - | - | - | - | - | Conduct ethical hacking (weight: 3)<br>Identify and solve cybersecurity-related issues (weight: 4) |
| **Man-in-the-middle attacks** | - | Conduct network configuration and setup (weight: 3) | - | - | - | - |
| **XML external entities (XXE)** | - | - | - | - | - | Conduct ethical hacking (weight: 3)<br>Identify and solve cybersecurity-related issues (weight: 4) |
| **Cryptojacking** | - | - | - | - | - | Decompose and analyse systems to identify weaknesses and ineffective controls (weight: 3)<br>Conduct ethical hacking (weight: 3) |
| **Watering hole** | - | - | - | - | - | Decompose and analyse systems to identify weaknesses and ineffective controls (weight: 3)<br>Conduct ethical hacking (weight: 3) |

| Identified threats | CYBERSECURITY EDUCATOR | CYBERSECURITY IMPLEMENTER | CYBERSECURITY RESEARCHER | CYBERSECURITY RISK MANAGER | DIGITAL FORENSICS INVESTIGATOR | PENETRATION TESTER |
|---|---|---|---|---|---|---|
| **INFORMATION TECHNOLOGY THREATS** | | | | | | |
| **Living off the land (LOTL)** | - | - | - | - | - | Decompose and analyse systems to identify weaknesses and ineffective controls (weight: 3)<br>Conduct ethical hacking (weight: 3) |
| **Insecure deserialization** | - | - | - | - | - | Conduct ethical hacking (weight: 3)<br>Identify and solve cybersecurity-related issues (weight: 4) |

### 5.2.3. Shared Information Technology Threats

Tables 10 and 11 offer a detailed mapping between Shared-IT threats ECSF role profiles. Within each table cell, a compilation of skills attributed to a specific job profile is provided, illustrating how these skills can be effectively employed to address and mitigate the Shared-IT security threats at hand.

The mapping of skills with respect to Shared IT threats also highlights several major skills from the ENISA cybersecurity skills framework. In particular, following and practicing auditing frameworks, standards and methodologies are essential for ensuring the enforcement of the security policy and maintaining secure and resilient infrastructures. This is required to properly address several cybersecurity threats, such as those affecting the supply chain or related to insider attacks. Collecting, analysing and correlating cyber threat information originating from multiple sources is also critical to address the lack of information sharing as well as deficiencies that may exist incident reporting activities. It may also address threats regarding third-party attacks or preventing some breakdown due to cybersecurity attacks. Coordinating the integration of security solutions is also a key requirement to guarantee the seamless integration of prevention, detection and mitigation methods and techniques used in an organization and minimise network infrastructures' attack surface. Educating, monitoring and assessing the awareness of organization members and external parties on cybersecurity and privacy issues is another important factor contributing to preventing low awareness with respect to security risks, and threats regarding compromised confidential or personal data. Analyzing and consolidating an organization's quality and risk management practices is another factor contributing to addressing threats with respect to resilience. These threats should also be addressed by regularly conducting performance and resilience test, to quantify an organisation's capabilities (technical and non-technical) to resist against successful attacks.

The analysis of this third mapping shows a relatively high coverage, with more than 80% of the shared Information Technology threats that are covered by at least two skills from the REWIRE skill framework. Again, some of the considered skills could be refined with respect to the specificities of cybersecurity threats. For instance, the threat regarding falsified and stolen medical data may require some refinements about medical information systems and their security, but also more generally about specific healthcare regulations. This contributes to a better handling of risks related to data falsification and data theft in a medical context. In the same manner, the threats regarding geopolitical instability risk could involve further specific skills with respect to monitoring and analysing geopolitical events, complying with international cybersecurity regulations, and even engaging in cyber diplomacy to mitigate inherent risks.

Overall, this mapping with respect to shared Information Technology threats highlights more specifically, amongst the 12 role profiles from the REWIRE skills framework, the following ones: the chief information security officer, the cyber threat intelligence specialist, the cybersecurity implementer, the cybersecurity auditor, and the cybersecurity implementer.

***Table 5. The skills and knowledge required to effectively mitigate Shared-IT threats for the first set of the ECSF role profiles***

| Identified threats | CHIEF INFORMATION SECURITY OFFICER (CISO) | CYBER INCIDENT RESPONDER | CYBER LEGAL, POLICY & COMPLIANCE OFFICER | CYBER SECURITY AUDITOR | CYBER THREAT INTELLIGENCE SPECIALIST | CYBERSECURITY ARCHITECT |
|---|---|---|---|---|---|---|
| **Shared-IT threats** | | | | | | |
| **Politically motivated attacks or hacktivism** | - | Recognize and categorize types of vulnerabilities and associated attacks (weight: 4) | - | Assess risk factors (weight: 4) | Collect, analyse and correlate cyber threat information originating from multiple sources (weight: 4) | - |
| **Unpatched & outdated software** | - | - | - | - | - | Coordinate the integration of security solutions (weight: 3) Monitor progress of issues throughout lifecycle and communicate effectively (weight: 3) |
| **Low awareness** | - | - | Educate, monitor and assess the awareness of organization members and external parties on cybersecurity and privacy issues as needed. (weight: 4) | - | - | - |
| **Lack of incident reporting** | - | Manage and analyse log files (weight: 3) Collect, analyse and correlate cyber threat information originating from | - | - | - | - |

| Identified threats | CHIEF INFORMATION SECURITY OFFICER (CISO) | CYBER INCIDENT RESPONDER | CYBER LEGAL, POLICY & COMPLIANCE OFFICER | CYBER SECURITY AUDITOR | CYBER THREAT INTELLIGENCE SPECIALIST | CYBERSECURITY ARCHITECT |
|---|---|---|---|---|---|---|
| **Shared-IT threats** | | | | | | |
| | | multiple sources (weight: 3) | | | | |
| **Lack of information sharing** | - | Manage and analyse log files (weight: 3)<br>Collect, analyse and correlate cyber threat information originating from multiple sources (weight: 3) | - | - | - | - |
| **Insider threats** | Communicate and promote the organisation's risk analysis outcomes and risk management processes (weight: 4) | - | - | - | - | - |
| **Risks of emerging technologies like blockchain, AI, VR, quantum computing, intelligent automation, etc** | Assist in communication of the enterprise architecture and standards, principles and objectives to the application teams (weight: 4)<br>Analyse and implement cybersecurity policies, certifications, standards, | - | Perform (Implement) and Monitor audits against cybersecurity-related applicable laws, regulations and standards, collect needed evidence and document audit information and results, in alignment to the relevant audit plan(s). (weight: 4) | Assess risk factors (weight: 4) | - | Coordinate the integration of security solutions (weight: 3) |

| Identified threats | CHIEF INFORMATION SECURITY OFFICER (CISO) | CYBER INCIDENT RESPONDER | CYBER LEGAL, POLICY & COMPLIANCE OFFICER | CYBER SECURITY AUDITOR | CYBER THREAT INTELLIGENCE SPECIALIST | CYBERSECURITY ARCHITECT |
|---|---|---|---|---|---|---|
| **Shared-IT threats** | | | | | | |
| | methodologies and frameworks (weight: 4) | | | | | |
| **Keeping up with changing regulatory requirements (e.g. GPDR, AI regulations, breach disclosure requirements etc.), or their ineffectiveness** | Assist in communication of the enterprise architecture and standards, principles and objectives to the application teams (weight: 3)<br>Analyse and implement cybersecurity policies, certifications, standards, methodologies and frameworks (weight: 4) | - | Perform (Implement) and Monitor audits against cybersecurity-related applicable laws, regulations and standards, collect needed evidence and document audit information and results, in alignment to the relevant audit plan(s). (weight: 4) | Follow and practice auditing frameworks, standards and methodologies (weight: 4)<br>Assess risk factors (weight: 3) | - | - |
| **Misinformation and disinformation sowing confusion among executives and the board about cyber risks** | Analyse and implement cybersecurity policies, certifications, standards, methodologies and frameworks (weight: 4) | Recognize and categorize types of vulnerabilities and associated attacks (weight: 3) | - | Follow and practice auditing frameworks, standards and methodologies (weight: 3) | Collect, analyse and correlate cyber threat information originating from multiple sources (weight: 4) | - |
| **Security misconfiguration** | Apply security design principles, e.g. least privilege (weight: 4) | - | - | - | - | - |

| Identified threats | CHIEF INFORMATION SECURITY OFFICER (CISO) | CYBER INCIDENT RESPONDER | CYBER LEGAL, POLICY & COMPLIANCE OFFICER | CYBER SECURITY AUDITOR | CYBER THREAT INTELLIGENCE SPECIALIST | CYBERSECURITY ARCHITECT |
|---|---|---|---|---|---|---|
| **Shared-IT threats** | | | | | | |
| **Third party related attacks** | Implement cybersecurity recommendations and best practices (weight: 4) | - | - | - | Collect, analyse and correlate cyber threat information originating from multiple sources (weight: 4)<br>Automate threat intelligence management procedures (weight: 3) | - |
| **Infrastructure breakdown due to cyberattack** | | Work on operating systems, servers, clouds and relevant infrastructures (weight: 4) | - | Follow and practice auditing frameworks, standards and methodologies (weight: 3)<br>Assess risk factors (weight: 4) | Automate threat intelligence management procedures (weight: 3) | Conduct performance and resilience testing (weight: 4) |
| **Geopolitical instability risk** | Apply security design principles, e.g. least privilege (weight: 4) | Collect, analyse and correlate cyber threat information originating from multiple sources (weight: 4) | - | Follow and practice auditing frameworks, standards and | - | - |

| Identified threats | CHIEF INFORMATION SECURITY OFFICER (CISO) | CYBER INCIDENT RESPONDER | CYBER LEGAL, POLICY & COMPLIANCE OFFICER | CYBER SECURITY AUDITOR | CYBER THREAT INTELLIGENCE SPECIALIST | CYBERSECURITY ARCHITECT |
|---|---|---|---|---|---|---|
| **Shared-IT threats** | | | | | | |
| | | | | methodologies (weight: 3) | | |
| **Supply-chain resilience** | Apply security design principles, e.g. least privilege (weight: 4) | Work on operating systems, servers, clouds and relevant infrastructures (weight: 2.5) | Perform (Implement) and Monitor audits against cybersecurity-related applicable laws, regulations and standards, collect needed evidence and document audit information and results, in alignment to the relevant audit plan(s). (weight: 4) | Assess risk factors (weight: 4) | Use and apply CTI platforms and tools (weight: 3) | Conduct performance and resilience testing (weight: 4.5) |
| **Blackmail due to compromised personal data** | - | - | Educate, monitor and assess the awareness of organization members and external parties on cybersecurity and privacy issues as needed. (weight: 3)<br>Enforce and advocate organisation's data privacy and protection program (weight: 4) | | Coordinate the integration of security solutions (weight: 3) | - |
| **Falsified or stolen medical data** | - | - | - | Follow and practice auditing frameworks, standards and methodologies (weight: 3) | Collect, analyse and correlate cyber threat information originating from multiple sources (weight: 4) | - |

***Table 6. The skills and knowledge required to effectively mitigate Shared-IT threats for the second set of the ECSF role profiles***

| Identified threats | CYBERSECURITY EDUCATOR | CYBERSECURITY IMPLEMENTER | CYBERSECURITY RESEARCHER | CYBERSECURITY RISK MANAGER | DIGITAL FORENSICS INVESTIGATOR | PENETRATION TESTER |
|---|---|---|---|---|---|---|
| **Shared IT threats** | | | | | | |
| **Politically motivated attacks or hacktivism** | - | - | - | Communicate, present and report to relevant stakeholders (weight: 4) | - | Perform social engineering (weight: 3) |
| **Unpatched & outdated software** | - | Develop code, scripts and programmes (weight: 4) | - | - | - | Develop code, scripts and programmes (weight: 4) |
| **Low awareness** | - | - | - | - | - | - |
| **Lack of incident reporting** | - | Communicate, present and report to relevant stakeholders (weight: 4) | - | Communicate, present and report to relevant stakeholders (weight: 4) | Collect information while preserving its integrity (weight: 4) Strictly and systematically follow the prescribed procedures. (weight: 3) | - |
| **Lack of information sharing** | - | Communicate, present and report to relevant stakeholders (weight: 4) | - | Communicate, present and report to relevant stakeholders (weight: 4) | Collect information while preserving its integrity (weight: 4) Strictly and systematically follow the | - |

| Identified threats | CYBERSECURITY EDUCATOR | CYBERSECURITY IMPLEMENTER | CYBERSECURITY RESEARCHER | CYBERSECURITY RISK MANAGER | DIGITAL FORENSICS INVESTIGATOR | PENETRATION TESTER |
|---|---|---|---|---|---|---|
| **Shared IT threats** | | | | | | |
| | | | | | prescribed procedures. (weight: 3) | |
| **Insider threats** | Monitor evolving security and privacy infrastructures, technologies and methods (weight: 4) | Performs basic risk assessments for small information systems. (weight: 3) | - | Build a cybersecurity risk-aware environment (weight: 4) | Work ethically and independently; not influenced and biased by internal or external actors (weight: 4) | - |
| **Risks of emerging technologies like blockchain, AI, VR, quantum computing, intelligent automation, etc** | - | Assess the security and performance of solutions (weight: 3) | - | Build a cybersecurity risk-aware environment (weight: 4) | - | - |
| **Keeping up with changing regulatory requirements (e.g. GPDR, AI regulations, breach disclosure requirements etc.), or their ineffectiveness** | - | | - | - | - | - |
| **Misinformation and disinformation sowing** | - | - | - | Identify sources of information that can be used for | - | - |

| Identified threats | CYBERSECURITY EDUCATOR | CYBERSECURITY IMPLEMENTER | CYBERSECURITY RESEARCHER | CYBERSECURITY RISK MANAGER | DIGITAL FORENSICS INVESTIGATOR | PENETRATION TESTER |
|---|---|---|---|---|---|---|
| **Shared IT threats** | | | | | | |
| **confusion among executives and the board about cyber risks** | | | | monitoring and measurement of cybersecurity controls. (weight: 2.5) | | |
| **Security misconfiguration** | - | Conduct network configuration and setup (weight: 3) | - | - | - | Decompose and analyse systems to identify weaknesses and ineffective controls (weight: 4)<br>Identify and solve cybersecurity-related issues (weight: 4) |
| **Third party related attacks** | - | - | - | - | - | - |
| **Infrastructure breakdown due to cyberattack** | - | Contribute to the identification of risks that arise from potential technical solution architectures. (weight: 3)<br>Suggest alternate solutions or countermeasures to mitigate risks. (weight: 3)<br>Define secure systems configurations in compliance with intended architectures (weight: 4) | Decompose and analyse systems to develop security and privacy requirements and identify effective solutions (weight: 3) | Oversee and control the implementation of prevention, security, and surveillance measures in order to assess their effectiveness and to make adjustments in case of unsatisfactory results. (weight: 4) | - | Decompose and analyse systems to identify weaknesses and ineffective controls (weight: 4) |
| **Geopolitical instability risk** | - | - | - | Analyse and consolidate | Recognize and categorize | Assess cybersecurity vulnerabilities (weight: 3) |

| Identified threats | CYBERSECURITY EDUCATOR | CYBERSECURITY IMPLEMENTER | CYBERSECURITY RESEARCHER | CYBERSECURITY RISK MANAGER | DIGITAL FORENSICS INVESTIGATOR | PENETRATION TESTER |
|---|---|---|---|---|---|---|
| **Shared IT threats** | | | | | | |
| | | | | organisation's quality and risk management practices (weight: 3) | types of vulnerabilities and associated attacks (weight: 3) | |
| **Supply-chain resilience** | - | - | - | Analyse and consolidate organisation's quality and risk management practices (weight: 3.5) | - | Assess cybersecurity vulnerabilities (weight: 3) |
| **Blackmail due to compromised personal data** | - | - | - | - | - | Identify and solve cybersecurity-related issues (weight: 3) |
| **Falsified or stolen medical data** | Monitor evolving security and privacy infrastructures, technologies and methods (weight: 3) | - | Decompose and analyse systems to develop security and privacy requirements and identify effective solutions (weight: 3) | - | - | - |

To sum up, this chapter has systematically aligned the predominant cybersecurity threats with the requisite skills delineated across the 12 ECSF role profiles. This mapping not only clarifies the direct relationships between emerging threats and the specific skill sets needed to counteract them but also reinforces the strategic importance of continuous skills development in the cybersecurity domain. The insights generated from this analysis are crucial for developing a proactive and resilient cybersecurity workforce, capable of adapting to the rapidly evolving digital threat landscape.

The REWIRE project has identified key cybersecurity threats and the skills needed to counter them. To close the cyber-skills gap, we've developed targeted training courses as part of our WP4 activities. These include Network Penetration Testing, Web Penetration Testing and Cyber-threat intelligence specialist, all directly aligned with the vulnerabilities discussed in this report. For example, our Network Penetration Testing course teaches professionals how to find and fix vulnerabilities in CMS platforms like WordPress and Drupal, addressing issues like DDoS attacks and outdated software. We also use the Social Engineering Toolkit (SET) to give hands-on experience in recognizing and defending against social engineering attacks, a growing concern in cybersecurity. Our Web Penetration Testing course focuses on preventing database breaches by teaching how to detect and guard against this serious web application vulnerability. Similarly, the Web Penetration Testing course covers essential areas like Cross-Site Scripting (XSS) and broken authentication, tackling common web security flaws head-on. The Cyber Threat Intelligence Specialist course addresses critical aspects of data privacy and securing sensitive information. It provides training on identifying, analyzing, and responding to cyber threats, with a strong focus on safeguarding data integrity and confidentiality. To improve information sharing, we've developed the CyberABILITY platform, a hub for sharing educational resources and best practices among cybersecurity professionals. By connecting these courses and tools to the specific threats identified, we ensure our training provides the practical skills needed to handle real-world cybersecurity challenges.

# CONCLUSIONS

The comprehensive analysis of job ads using the Job Ads Analyzer, in conjunction with the cybersecurity threat reports and the skills required to address them, presents a clear picture of the current cybersecurity job market and its alignment with the prevailing cyber threats. The ENISA report underscores the persistent nature of certain cyber threats such as ransomware, malware, social engineering, and supply-chain attacks. The job market analysis through the Job Ads Analyzer indicates that there is a significant demand for a wide range of skills to counter these threats.

The job ads reflect the demand for roles that can address the specific threats identified in the ENISA report. High-demand roles such as *Cybersecurity Implementer*, *Cybersecurity Architect*, and *Incident Responder*, *Chief Information Security Officer* and *Cybersecurity risk manager* indicate a market leaning towards operational and architectural expertise, which aligns with the need to develop robust defences against complex cybersecurity challenges. The number of job ads for each role provides an indication of the market's valuation of the skills necessary to address specific threats, and subsequently, where training and development efforts may be beneficial.

From the skills perspective, the cybersecurity job market is currently emphasizing a diverse range of skills that include both technical expertise and soft skills. Leading the demand is the ability to 'Collaborate and Communicate,' underscoring the importance of interpersonal skills in managing and conveying complex cybersecurity issues effectively across various stakeholders. Technical skills related to 'Information Systems and Network Security' and 'Information Security Controls Assessment' are also highly sought after, reflecting the need for professionals who can secure networks and assess as well as implement security controls.

In conclusion, the findings suggest that the cybersecurity job market is closely aligned with the current threat environment, emphasizing the need for professionals who are not only technically proficient but also adept in communication and strategic planning. The REWIRE project's focus on developing curricula and certifications for specific roles will address these needs, aiming to provide a better understanding of the situation in the cybersecurity skills market and enhance the workforce's ability to effectively respond to cyber threats.

# REFERENCES

[i] Ricci S, Sikora M, Parker S, Lendak I, Danidou Y, Chatzopoulou A, Badonnel R, Alksnys D., "Job Adverts Analyzer for Cybersecurity Skills Needs Evaluation.," in ARES - 17th International Conference on Availability, Reliability and Security 2022, Vienna, 2022
[ii] Briones, A., Ricci, S., Chatzopoulou, A., Cegan, J., Dzurenda, P., Koutoudis, I., Enhancing Cybersecurity Education in Europe: The REWIRE's Course Selection Methodology in ARES - 18th International Conference on Availability, Reliability and Security 2023, Benevento, 2023
[iii] ENISA Threat Landscape 2023, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
[iv] UK NCSC Annual Review 2022, https://www.ncsc.gov.uk/files/NCSC-Annual-Review-2022.pdf
[v] UK NCSC Annual Review 2022, https://www.ncsc.gov.uk/files/NCSC-Annual-Review-2022.pdf
[vi] Australian Cyber Security Centre Annual Cyber Threat Report 2022, https://www.cyber.gov.au/sites/default/files/2023-03/ACSC-Annual-Cyber-Threat-Report-2022_0.pdf
[vii] Australian Cyber Security Centre Annual Cyber Threat Report 2022, https://www.cyber.gov.au/sites/default/files/2023-03/ACSC-Annual-Cyber-Threat-Report-2022_0.pdf
[viii] Australian Cyber Security Centre Annual Cyber Threat Report 2022, https://www.cyber.gov.au/sites/default/files/2023-03/ACSC-Annual-Cyber-Threat-Report-2022_0.pdf
[ix] Australian Cyber Security Centre Annual Cyber Threat Report 2022, https://www.cyber.gov.au/sites/default/files/2023-03/ACSC-Annual-Cyber-Threat-Report-2022_0.pdf
[x] The CrowdStrike 2023 Global Threat Report, https://www.crowdstrike.com/global-threat-report/
[xi] Sophos 2023 threat trend report, https://www.sophos.com/en-us/content/security-threat-report
[xii] Sophos 2023 threat trend report, https://www.sophos.com/en-us/content/security-threat-report
[xiii] Sophos 2023 threat trend report, https://www.sophos.com/en-us/content/security-threat-report
[xiv] Sophos 2023 threat trend report, https://www.sophos.com/en-us/content/security-threat-report
[xv] The CrowdStrike 2023 Global Threat Report, https://www.crowdstrike.com/global-threat-report/
[xvi] New-Zealand National Cyber Security Centre report 2021/2022, https://www.ncsc.govt.nz/news/cyber-threat-report-for-20212022-released/
[xvii] Truesec Threat Intelligence Report 2023, https://www.truesec.com/hub/report/threat-intelligence-report-2023;

[xviii] The CrowdStrike 2023 Global Threat Report, https://www.crowdstrike.com/global-threat-report/
[xix] The CrowdStrike 2023 Global Threat Report, https://www.crowdstrike.com/global-threat-report/
[xx] Truesec Threat Intelligence Report 2023, https://www.truesec.com/hub/report/threat-intelligence-report-2023;
[xxi] The CrowdStrike 2023 Global Threat Report, https://www.crowdstrike.com/global-threat-report/
[xxii] The CrowdStrike 2023 Global Threat Report, https://www.crowdstrike.com/global-threat-report/
[xxiii] The CrowdStrike 2023 Global Threat Report, https://www.crowdstrike.com/global-threat-report/
[xxiv] Truesec Threat Intelligence Report 2023, https://www.truesec.com/hub/report/threat-intelligence-report-2023;
[xxv] UK NCSC Annual Review 2022, https://www.ncsc.gov.uk/files/NCSC-Annual-Review-2022.pdf
[xxvi] ENISA Threat Landscape 2023, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
[xxvii] ENISA Threat Landscape for Supply Chain Attacks, https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks
[xxviii] New-Zealand National Cyber Security Centre report 2021/2022, https://www.ncsc.govt.nz/news/cyber-threat-report-for-20212022-released/
[xxix] New-Zealand National Cyber Security Centre report 2021/2022, https://www.ncsc.govt.nz/news/cyber-threat-report-for-20212022-released/
[xxx] New-Zealand National Cyber Security Centre report 2021/2022, https://www.ncsc.govt.nz/news/cyber-threat-report-for-20212022-released/; The CrowdStrike 2023 Global Threat Report, https://www.crowdstrike.com/global-threat-report/; Sophos 2023 threat trend report, https://www.sophos.com/en-us/content/security-threat-report; Truesec Threat Intelligence Report 2023, https://www.truesec.com/hub/report/threat-intelligence-report-2023
[xxxi] The CrowdStrike 2023 Global Threat Report, https://www.crowdstrike.com/global-threat-report/
[xxxii] New-Zealand National Cyber Security Centre report 2021/2022, https://www.ncsc.govt.nz/news/cyber-threat-report-for-20212022-released/
[xxxiii] New-Zealand National Cyber Security Centre report 2021/2022, https://www.ncsc.govt.nz/news/cyber-threat-report-for-20212022-released/
[xxxiv] Briones, A., Ricci, S., Chatzopoulou, A., Cegan, J., Dzurenda, P., Koutoudis, I., Enhancing Cybersecurity Education in Europe: The REWIRE's Course Selection Methodology in ARES - 18th International Conference on Availability, Reliability and Security 2023, Benevento, 2023
[xxxv] ENISA Threat Landscape 2023, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

[xxxvi] UK NCSC Annual Review 2022, https://www.ncsc.gov.uk/files/NCSC-Annual-Review-2022.pdf
[xxxvii] UK NCSC Annual Review 2022, https://www.ncsc.gov.uk/files/NCSC-Annual-Review-2022.pdf
[xxxviii] Australian Cyber Security Centre Annual Cyber Threat Report 2022, https://www.cyber.gov.au/sites/default/files/2023-03/ACSC-Annual-Cyber-Threat-Report-2022_0.pdf
[xxxix] Australian Cyber Security Centre Annual Cyber Threat Report 2022, https://www.cyber.gov.au/sites/default/files/2023-03/ACSC-Annual-Cyber-Threat-Report-2022_0.pdf
[xl] Australian Cyber Security Centre Annual Cyber Threat Report 2022, https://www.cyber.gov.au/sites/default/files/2023-03/ACSC-Annual-Cyber-Threat-Report-2022_0.pdf
[xli] Australian Cyber Security Centre Annual Cyber Threat Report 2022, https://www.cyber.gov.au/sites/default/files/2023-03/ACSC-Annual-Cyber-Threat-Report-2022_0.pdf
[xlii] The CrowdStrike 2023 Global Threat Report, https://www.crowdstrike.com/global-threat-report/
[xliii] Sophos 2023 threat trend report, https://www.sophos.com/en-us/content/security-threat-report
[xliv] Sophos 2023 threat trend report, https://www.sophos.com/en-us/content/security-threat-report
[xlv] Sophos 2023 threat trend report, https://www.sophos.com/en-us/content/security-threat-report
[xlvi] Sophos 2023 threat trend report, https://www.sophos.com/en-us/content/security-threat-report
[xlvii] The CrowdStrike 2023 Global Threat Report, https://www.crowdstrike.com/global-threat-report/
[xlviii] New-Zealand National Cyber Security Centre report 2021/2022, https://www.ncsc.govt.nz/news/cyber-threat-report-for-20212022-released/
[xlix] Truesec Threat Intelligence Report 2023, https://www.truesec.com/hub/report/threat-intelligence-report-2023;
[l] The CrowdStrike 2023 Global Threat Report, https://www.crowdstrike.com/global-threat-report/
[li] The CrowdStrike 2023 Global Threat Report, https://www.crowdstrike.com/global-threat-report/
[lii] Truesec Threat Intelligence Report 2023, https://www.truesec.com/hub/report/threat-intelligence-report-2023;
[liii] The CrowdStrike 2023 Global Threat Report, https://www.crowdstrike.com/global-threat-report/
[liv] The CrowdStrike 2023 Global Threat Report, https://www.crowdstrike.com/global-threat-report/

[lv] The CrowdStrike 2023 Global Threat Report, https://www.crowdstrike.com/global-threat-report/
[lvi] Truesec Threat Intelligence Report 2023, https://www.truesec.com/hub/report/threat-intelligence-report-2023;
[lvii] UK NCSC Annual Review 2022, https://www.ncsc.gov.uk/files/NCSC-Annual-Review-2022.pdf
[lviii] ENISA Threat Landscape 2023, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
[lix] ENISA Threat Landscape for Supply Chain Attacks, https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks
[lx] New-Zealand National Cyber Security Centre report 2021/2022, https://www.ncsc.govt.nz/news/cyber-threat-report-for-20212022-released/
[lxi] New-Zealand National Cyber Security Centre report 2021/2022, https://www.ncsc.govt.nz/news/cyber-threat-report-for-20212022-released/
[lxii] New-Zealand National Cyber Security Centre report 2021/2022, https://www.ncsc.govt.nz/news/cyber-threat-report-for-20212022-released/; The CrowdStrike 2023 Global Threat Report, https://www.crowdstrike.com/global-threat-report/; Sophos 2023 threat trend report, https://www.sophos.com/en-us/content/security-threat-report; Truesec Threat Intelligence Report 2023, https://www.truesec.com/hub/report/threat-intelligence-report-2023
[lxiii] The CrowdStrike 2023 Global Threat Report, https://www.crowdstrike.com/global-threat-report/
[lxiv] New-Zealand National Cyber Security Centre report 2021/2022, https://www.ncsc.govt.nz/news/cyber-threat-report-for-20212022-released/
[lxv] New-Zealand National Cyber Security Centre report 2021/2022, https://www.ncsc.govt.nz/news/cyber-threat-report-for-20212022-released/
[lxvi] Briones, A., Ricci, S., Chatzopoulou, A., Cegan, J., Dzurenda, P., Koutoudis, I., Enhancing Cybersecurity Education in Europe: The REWIRE's Course Selection Methodology in ARES - 18th International Conference on Availability, Reliability and Security 2023, Benevento, 2023
[lxvii] ENISA Threat Landscape 2023, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
[lxviii] UK NCSC Annual Review 2022, https://www.ncsc.gov.uk/files/NCSC-Annual-Review-2022.pdf
[lxix] UK NCSC Annual Review 2022, https://www.ncsc.gov.uk/files/NCSC-Annual-Review-2022.pdf
[lxx] Australian Cyber Security Centre Annual Cyber Threat Report 2022, https://www.cyber.gov.au/sites/default/files/2023-03/ACSC-Annual-Cyber-Threat-Report-2022_0.pdf
[lxxi] Australian Cyber Security Centre Annual Cyber Threat Report 2022, https://www.cyber.gov.au/sites/default/files/2023-03/ACSC-Annual-Cyber-Threat-Report-2022_0.pdf

[lxxii] Australian Cyber Security Centre Annual Cyber Threat Report 2022, https://www.cyber.gov.au/sites/default/files/2023-03/ACSC-Annual-Cyber-Threat-Report-2022_0.pdf
[lxxiii] Australian Cyber Security Centre Annual Cyber Threat Report 2022, https://www.cyber.gov.au/sites/default/files/2023-03/ACSC-Annual-Cyber-Threat-Report-2022_0.pdf
[lxxiv] The CrowdStrike 2023 Global Threat Report, https://www.crowdstrike.com/global-threat-report/
[lxxv] Sophos 2023 threat trend report, https://www.sophos.com/en-us/content/security-threat-report
[lxxvi] Sophos 2023 threat trend report, https://www.sophos.com/en-us/content/security-threat-report
[lxxvii] Sophos 2023 threat trend report, https://www.sophos.com/en-us/content/security-threat-report
[lxxviii] Sophos 2023 threat trend report, https://www.sophos.com/en-us/content/security-threat-report
[lxxix] The CrowdStrike 2023 Global Threat Report, https://www.crowdstrike.com/global-threat-report/
[lxxx] New-Zealand National Cyber Security Centre report 2021/2022, https://www.ncsc.govt.nz/news/cyber-threat-report-for-20212022-released/
[lxxxi] Truesec Threat Intelligence Report 2023, https://www.truesec.com/hub/report/threat-intelligence-report-2023;
[lxxxii] The CrowdStrike 2023 Global Threat Report, https://www.crowdstrike.com/global-threat-report/
[lxxxiii] The CrowdStrike 2023 Global Threat Report, https://www.crowdstrike.com/global-threat-report/
[lxxxiv] Truesec Threat Intelligence Report 2023, https://www.truesec.com/hub/report/threat-intelligence-report-2023;
[lxxxv] The CrowdStrike 2023 Global Threat Report, https://www.crowdstrike.com/global-threat-report/
[lxxxvi] The CrowdStrike 2023 Global Threat Report, https://www.crowdstrike.com/global-threat-report/
[lxxxvii] The CrowdStrike 2023 Global Threat Report, https://www.crowdstrike.com/global-threat-report/
[lxxxviii] Truesec Threat Intelligence Report 2023, https://www.truesec.com/hub/report/threat-intelligence-report-2023;
[lxxxix] UK NCSC Annual Review 2022, https://www.ncsc.gov.uk/files/NCSC-Annual-Review-2022.pdf
[xc] ENISA Threat Landscape 2023, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
[xci] ENISA Threat Landscape for Supply Chain Attacks, https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

[xcii] New-Zealand National Cyber Security Centre report 2021/2022, https://www.ncsc.govt.nz/news/cyber-threat-report-for-20212022-released/
[xciii] New-Zealand National Cyber Security Centre report 2021/2022, https://www.ncsc.govt.nz/news/cyber-threat-report-for-20212022-released/