2024 REPORT ON THE STATE OF CYBERSECURITY IN THE UNION PANEL SERIES

ADVANCING THE EUROPEAN CYBERSECURITY SKILLS FRAMEWORK AND IMPLEMENTING THE EU CYBERSECURITY SKILLS ACADEMY ACROSS MEMBER STATES - EXPERTS PERSPECTIVES

1. INTRODUCTION

In December 2024, the European Union Agency for Cybersecurity (ENISA) released the 2024 Report on the State of Cybersecurity in the Union, adopted in cooperation with the European Commission and the Network and Information Systems Cooperation Group (NS CG), gathering all EU Member States to cooperate on cybersecurity strategic matters. The Report provides an in-depth analysis of current challenges and opportunities for strengthening cybersecurity in the European Union. ENISA is organising a series of policy panels at key cybersecurity conferences throughout 2025, with the aim to dive deeper into the Report's six key recommendations and foster discussions on the steps required to implement them.

On 3rd April 2025, the SECURE International Summit in Poland hosted a panel on cybersecurity skills, a crucial element for building long-term resilience against cyber threats.

This paper presents the main discussion points and conclusions.

2. BACKGROUND

2024 State of Cybersecurity Report: Problem Statement

- Organisations are struggling to find qualified cybersecurity professionals. The 2024 Eurobarometer survey on cyber skills shows that **47% of 12,000 surveyed organizations** report difficulties in hiring suitable candidates.
- NIS Investment study from 2023 reports that nearly **half of Operators of Essential Services (OESs) and Digital Service Providers (DSPs) under NIS1** plan to hire **an average of four** full-time cybersecurity professionals (FTEs) within the next two years
- The CyberHead Education Database reveals that only **20% of cybersecurity graduates are women**, limiting gender balance in the workforce.

In response to the identified challenges, the Report includes the following recommendations:

- **Implementing the EU Cybersecurity Skills Academy** as a central hub for workforce development.
- **Establishing a common EU approach to cybersecurity training** to ensure consistency and quality across member states.
- **Identifying future cybersecurity skills** needs to align training programs with emerging threats and technologies.
- **Developing a coordinated EU approach to stakeholder involvement** (governments, industry, academia) to address the cybersecurity skills gap.
- **Setting up a European attestation scheme** for validating and recognizing cybersecurity skills across the EU.

3. KEY INSIGHTS

Panel Title: Advancing the European Cybersecurity Skills Framework and Implementing the EU Cybersecurity Skills Academy across Member States

Moderator: Fabio Di Franco, ENISA
Panelists:

- Sergio Tringali, Information Systems Audit and Control Association (ISACA)
- Tiina Pau, Estonian Information System Authority (RIA)
- Hector Laiz Ibáñez, the Spanish National Cybersecurity Institute (INCIBE)

The value of the European Cybersecurity Skills Framework (ECSF)

The panelists agreed that the ECSF is a foundational tool for shaping cybersecurity roles and career pathways across the EU. The framework establishes a **common taxonomy and language** for cybersecurity roles, supporting businesses, academia, and governments alike. It is aligned with **recognised international standards**, ensuring relevance and interoperability.

Additionally, the ECSF promotes **harmonisation across Member States**, reducing fragmentation in how cybersecurity roles are defined and understood. Importantly, the ECSF also facilitates **intra-EU labor mobility**, helping professionals move and work across borders.

The ECSF significantly boosts employment and employability in cybersecurity roles across the EU. It helps simplify the recognition of cybersecurity competencies, which enhances the design of training programs and supports long-term career development.

European attestation scheme for skills

The panel welcomed the idea of a **European attestation scheme for cybersecurity skills,** recognising it as a crucial step toward **validating professional competencies** across the EU. Panelists emphasized the importance of **integrating existing professional certifications and trusted training programs** into the scheme to avoid duplication. A well-implemented attestation scheme would increase workforce mobility and provide clear pathways into cybersecurity careers.

A standardised terminology and assessment methodology, under an EU-wide governance model, would enable better alignment between businesses and professionals, supporting uptake of cybersecurity roles by providing greater clarity and confidence to employers and job seekers alike.

National perspectives:

Estonia
In Estonia, a recently published monitoring report shows that **25% of new employees in IT and cybersecurity are coming from outside the country**. This highlights the **importance of a common attestation scheme that is widely accepted by Member States**, as it facilitates workforce mobility across borders.

The Estonian cybersecurity strategy identifies two primary **workforce challenges: a shortage of experts and the need for highly skilled specialists in specific domains**. Increasing female participation in the sector is seen as a growth opportunity. One of the most impactful solutions identified is rooted in general education. The strategy seeks to integrate both cybersecurity hygiene and an awareness of cybersecurity as a viable career path into all levels of the general education system.

Spain
The Spanish representative offered a **comprehensive example of how Member States can proactively address cybersecurity skills challenges at the national level**. The Spanish National Cybersecurity Institute (INCIBE), in collaboration with National Observatory of Technology and Society (ONTSI), conducted a detailed workforce monitoring and diagnostics study titled "Análisis y Diagnóstico del Talento en Ciberseguridad en España" (2022). The study projected a demand for over 83,000 cybersecurity professionals by 2024 and has since guided several targeted initiatives, including bootcamps and scholarship programs.

Spain also places **strong emphasis on diversity and inclusion**, **actively promoting gender diversity in STEM fields** in line with recommendations from the Global Gender Gap Report 2023. Initiatives such as Women for Technical Talks (W4TT), Empresa Nacional de Innovación S.A., and the national Ciencia en Igualdad plan exemplify efforts to support women and foster digital entrepreneurship. In addition, INCIBE runs **inclusive training programs designed for underrepresented groups and individuals with disabilities**. Nearly 1,000 professionals have been trained through these efforts, helping to cultivate a more diverse and resilient cybersecurity workforce.

Workforce Trends: Insights from ISACA

According to the 2024 ISACA analysis, **demand for cybersecurity professionals is growing at a rate of 15–25% annually**, while **supply is increasing by only 6–8%**. **62% of organizations** have unfilled cybersecurity positions, with **60% struggling to retain talent**. A key challenge lies in the **narrow perception of qualifications** - many still assume that only software engineers are suited for cybersecurity roles. In reality, individuals with **diverse**

academic and professional backgrounds can succeed in the field, provided they receive the appropriate training and support.

Public-Private Collaboration & Community Building

The panel emphasised the importance of **public-private partnerships** and p**an-European collaboration** in addressing the cybersecurity skills gap. The **Cybersecurity Skills Academy**, which is a European policy initiative, part of the 2023 European Year of Skills was praised for uniting EU-level efforts, pledges, and raising visibility around workforce challenges. While the Academy has made significant strides, panellists agreed that even greater public-private collaboration is essential to meet the EU's 2030 workforce targets.

Despite ongoing progress, **the current pace of workforce development is insufficient** to meet the **growing demand** for securing national infrastructures and services. **Annual skills conferences and shared platforms** continue to play a key role in facilitating knowledge exchange across Member States. Sustained **stakeholder coordination**, between governments, academia, and industry, is critical to long-term success.

4. CONCLUSIONS

This panel underlined the urgency of closing the cybersecurity skills gap in the EU and emphasized the **pivotal role** of the European Cybersecurity Skills Framework and the EU Cybersecurity Skills Academy in this effort. Key themes that emerged included **harmonization**, **professional mobility**, **skills validation**, and **inclusion**. To meet EU's digital security goals by 2030, **strategic coordination and scalable actions at both EU and national levels are essential**.