CYBERSEC
EXPO & FORUM

SKILLS AND CYBER HYGIENE – SUPPORT AND DEVELOPMENT OF DIGITAL COMPETENCES

POLICY BRIEF

Table of contents

Dear Ladies and Gentlemen,

During **CYBERSEC EXPO & FORUM 2024**, on June 19 in Kraków, in the presence of Deputy Prime Minister and Minister of Digital Affairs Krzysztof Gawkowski, a letter of intent was signed between the Kościuszko Institute and the European Cybersecurity Organization (ECSO) regarding the organization of a series of events dedicated to the digital and technological policy priorities of Poland's presidency in the Council of the EU.

The initiative aims to support Poland's presidency in achieving goals related to cybersecurity and new technologies, strengthen cross-sectoral dialogue on digital challenges, and engage diverse stakeholders in shaping public policies, contributing to the development of specific strategies and solutions.

In the face of rapid digitization and growing cybersecurity challenges, digital competencies and awareness of cyber hygiene principles are essential foundations for the stable development of an information society. This document, prepared for the Ministry of Digital Affairs, includes recommendations for actions aimed at identifying gaps, increasing the level of knowledge and skills in the safe use of digital technologies in Poland. These recommendations are based on the expertise and experience of professionals and the results of analyses of key challenges in the areas of digital skills and cyber hygiene, identified by a working group comprising of experts from the public sector, representatives of the European Cybersecurity Organization (ECSO), the private sector, and educational institutions.

The work on the policy brief is aligned with the Strategy for the Development of Digital Competencies for 2025-2035, published by the Ministry of Digital Affairs, and incorporates Poland's key priorities stemming from its undertaking of the presidency of the Council of the European Union.

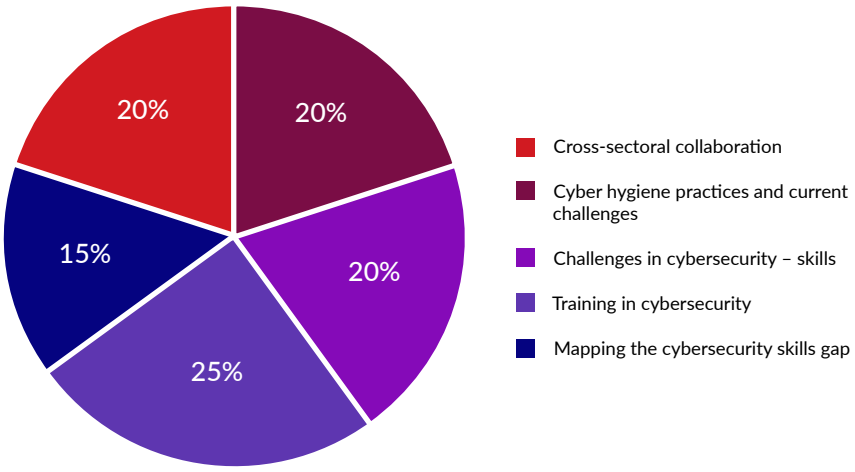
The developed recommendations will contribute to achieving community goals, such as building a secure and digitally resilient Europe, through the development of tools for support and education in the field of cybersecurity.

This document includes proposals for specific actions designed to help implement the Ministry's strategy, ensuring that society and institutions gain awareness and preparedness for the challenges of the digital future and acquire the ability to effectively protect their resources and data in an increasingly complex digital environment.

The policy brief has been divided into five areas:

1. Challenges in cybersecurity – skills
2. Mapping the cybersecurity skills gap
3. Training in cybersecurity
4. Cyber hygiene practices and current challenges
5. Cross-sectoral collaboration

Share of the main areas of recommendation



We would like to express our heartfelt gratitude to all members of the working group whose dedication, knowledge, and experience contributed to the creation of this document. The developed recommendations represent a significant step in building a digital and secure society. We extend our sincere thanks to the Ministry of Digital Affairs for their invaluable support and commitment, which played a crucial role in the realization of our initiative. We greatly appreciate your professionalism, openness to cooperation, meaningful contributions, and support of our shared mission.

Members of the working group:

1. Dr. Eng. Jędrzej Bieniasz – Cybersecurity Center, Warsaw University of Technology
2. Wojciech Bobak – National-Louis University, School of Business
3. Ivan Bornacelly – OECD Centre for Skills
4. Beata Chodacka – AGH University of Science and Technology in Kraków
5. Marietta Gieroń – The Kościuszko Institute
6. Kayle Giroud – Global Cyber Alliance
7. Paulina Górska – The Kościuszko Institute
8. Sid Hollman – Digital Europe
9. Karol Jędrasiak – GETES Institute
10. Łukasz Jędrzejczak – Deloitte
11. Katarzyna Nowak – Ministry of Digital Affairs
12. płk dr Piotr Potejko – University of Warsaw
13. Michał Pukaluk – Ministry of Digital Affairs
14. Krzysztof Sierański – Information Security Foundation
15. Alek Tarkowski – Open Future Foundation
16. Mariusz Ustyjańczuk – Deloitte
17. Martyna Wilk – Wrocław Center for Social Development
18. Katarzyna Wójtowicz-Garcarz – GETES Institute

We also extend our sincerest gratitude **to all partner institutions and experts** who supported the substantive and organizational efforts.

TOPIC I:

Challenges in cybersecurity – skills

Skills in the field of cybersecurity are critical today for the effective functioning of society and the economy, yet the skills gap in this area poses a significant challenge. There is a shortage of specialists, a lack of basic digital education, and technological exclusion among various social groups, all of which require urgent action. Cybersecurity is not just about system protection but also about developing practical skills, critical thinking, and resilience against misinformation. Investments in education, harmonized certification programs, and cross-sector collaboration are essential to build a resilient society capable of meeting the challenges of the digital reality.

CHALLENGES AND RECOMMENDATIONS

CHALLENGES

The European Union is currently facing a shortage of approximately 3 million cybersecurity specialists, with Poland also experiencing a significant skills gap in this area. The gap encompasses both technical and soft skills, posing a significant challenge for the labor market. The situation is further exacerbated by the emigration of experts abroad and fundamental educational shortcomings in society, requiring a comprehensive, society-wide approach.

At the same time, there is a visible lack of basic knowledge about digital hygiene and practical skills, such as understanding data structures or the principles of safe information sharing. To address these gaps, employers are increasingly opting for workplace training and coaching as effective methods of developing the required skills.

The digital skills gap problem affects not only the technology sector but society as a whole. Many people still lack basic computer skills or knowledge of software such as Microsoft Office. While foundations and non-governmental organizations run programs aimed at raising awareness of cybersecurity and digital competencies, more fundamental deficiencies in knowledge and skills are evident in practice. A lack of motivation to address these deficiencies further deepens digital exclusion.

Paradoxically, the rapid development of technology has not narrowed the gap but has instead widened it. Individuals with deficits in digital skills, particularly older adults, face increasing difficulties in compensating for these deficiencies. Digital exclusion is especially pronounced in the 60+ age group, where skills are often limited to basic computer use, and access to development opportunities remains restricted.

Generational differences in attitudes toward technology further reinforce these inequalities. Older generations often show a lack of trust in technology and difficulties in adapting to it, while younger generations, despite growing up in a digital environment, often lack critical information analysis skills and resilience to misinformation. These discrepancies lead to misconceptions and myths, reinforcing intergenerational barriers and hampering the development of necessary digital skills in society.

RECOMMENDATIONS

1. Establish a comprehensive catalog of skills encompassing both soft and technical digital competencies. This process should support continuous skill development and promote the idea of lifelong learning. It is essential to precisely define the range of competencies expected of graduates to meet current labor market needs. This catalog should be developed in collaboration with business representatives to align it with evolving professional requirements. Graduates should not only possess basic digital skills but also be prepared to operate in rapidly changing technological conditions. The systematization of graduate profiles and a clearly defined skill set are crucial for preparing individuals to meet the challenges of the modern world. The European Union can play a significant role as a natural platform for collaboration in establishing unified standards for digital competencies.

2. Education programs should combine digital and soft skills, such as critical thinking, situation analysis, and problem-solving. A structural approach to teaching is necessary, focusing on understanding system processes and technology operations rather than simply using specific tools. The inclusion of cybersecurity education from an early stage, promoting awareness and skills development in youth, is essential. The education system should integrate formal university pathways with informal training, ensuring mutual reinforcement of certifications and academic studies. Adapting training programs to changing labor market needs requires close collaboration with employers, policymakers, and educational institutions. Introducing a minimum curriculum on digital hygiene, with effective implementation and enforcement, is a priority for building an informed society. Additionally, public awareness and education campaigns should build trust and emphasize the importance of IT and cybersecurity education. A cross-disciplinary approach combining soft and hard skills provides a solid foundation for modern educational programs and addresses the needs of the changing job market. Developing an educational strategy supporting digital competencies at local and national levels, including collaboration with local governments, is essential for bridging the skills gap.

3. Increase access to junior positions, internships, and workshops focused on practical experience rather than requiring extensive certifications. Create environments that support retraining and skill-building, such as workshops and dedicated training sessions. A shift in narrative is also needed— cybersecurity should be framed as a space for learning and development rather than a narrow specialization. Employers should revise their qualification requirements, focusing on practical skills like project portfolios or practical tests rather than formal references. Micro-certifications, online courses, and other alternative qualifications should be more widely appreciated.

4. Encourage individuals from non-technical fields to transition into cybersecurity and include those with non-technical skills who can develop their competencies on the job. Emphasize the value of soft skills, such as critical thinking and project management, in cybersecurity. Diverse teams perform better, a fact that should be highlighted in promotional and informational campaigns.

5. Avoid stereotypical advertising campaigns, such as „You too can work in IT," which ignore the existing experience and skills of potential female candidates, often having a counterproductive effect. Implement programs supporting women in IT, such as training in incident detection.

6. Consider creating an educational platform, within the M-Obywatel application for example, to serve as an informational and educational space. This initiative could raise awareness of fraud methods targeting seniors, teach recognition of credible information sources, and combat misinformation. Particular attention should be given to addressing the inadequate digital skills of older generations, supporting their adaptation to the rapid pace of technological development. These efforts could include creating educational spaces related to cybersecurity, building trust in technology, and emphasizing the importance of collaboration for online safety. Strengthening community empowerment and implementing intergenerational programs to overcome barriers and integrate age groups around shared educational goals are essential. At the same time, efforts should counter „cyber resistance"—an aversion to learning new digital competencies that have become essential in daily life and the digital reality. Systematic monitoring and analysis of activities in cyberspace will allow better shaping of its development. Consistent support in learning and openness to new technologies will help create an informed and resilient digital society.

7. Policymakers play a crucial role in creating conditions conducive to the development of digital and professional competencies. It is necessary to ensure stable and adequate funding, support regulations that allow greater flexibility in education and employment, and promote EU-recognized certification standards.

These actions should align with a long-term labor market development strategy, accounting for technological changes and the needs of various social groups. Non-governmental organizations can play a significant role in organizing training and certification for ICT experts, particularly in digitally excluded areas. To fully leverage their potential, financial support and appropriate legal frameworks facilitating cross-sector collaboration are essential. Such cooperation could include public-private partnerships to utilize available resources effectively and introduce innovative solutions. Additionally, attention should be given to developing educational programs for disadvantaged groups, such as older adults, women entering the ICT job market, or youth in regions with limited access to modern technologies. It is also critical to invest in initiatives that promote awareness of the importance of digital competencies in daily life, both professionally and socially. Building societal awareness, supporting local leaders, and motivating young people to engage in the ICT sector can contribute to a more sustainable and resilient labor market prepared for future challenges.

8. Establish unified European certification programs covering both technical and soft skills essential in modern workplaces. These certifications, recognized across the European Union, can create a consistent qualification assessment system, facilitating the mobility of specialists between member states. A key aspect of this approach is the development of practical educational programs in collaboration with employers. Practical training in real working conditions and the promotion of recognizable certifications can encourage broader social groups to pursue cybersecurity and other IT fields. Certifications verifying specific skills provide opportunities for individuals with talent and motivation to develop, even without traditional academic backgrounds. This approach enables the recruitment of new employees with diverse competency profiles. Additionally, modular education pathways should be developed, allowing for gradual qualification acquisition tailored to individual needs and capabilities. Such a system promotes flexibility, facilitates balancing work and study, and increases access to education for individuals from disadvantaged regions or with limited access to traditional forms of learning. Moreover, the development of harmonized certification programs can significantly reduce barriers to entering the labor market. Transparency and recognition of qualifications at the European level will enable employers to assess candidates' competencies more quickly and learners to align more easily with market requirements. Investing in such solutions also supports inclusivity, allowing more people to grow in the IT and cybersecurity fields, which in the long term can help reduce the shortage of specialists in these areas. Ultimately, these actions should be part of a broader strategy, encompassing not only certification implementation but also promoting international collaboration, supporting innovative teaching methods, and raising societal awareness of the importance of digital competencies for the future labor market.

TOPIC II:

Mapping the cybersecurity skills gap

Mapping the cybersecurity skills gap involves identifying areas where appropriate skills are lacking in order to meet the demands of a rapidly developing digital reality. In the face of the dynamic advancement of technology and the rapidly changing digital environment, it is crucial to undertake actions aimed at understanding critical areas of deficit. Effective mapping allows for the assessment of the scale of problems and the identification of necessary steps to address them, supporting workforce development, and increasing the digital resilience of organizations and society.

CHALLENGES AND RECOMMENDATIONS

CHALLENGES

The cybersecurity industry faces numerous challenges stemming from a shortage of qualified personnel. The demand for experts with technical skills, such as cloud security, information and network system protection, data privacy assurance, threat analysis, and incident management, is growing significantly. Key roles requiring these qualifications include Chief Information Security Officer (CISO), Cybersecurity Implementer, and Cyber Incident Responder.

Many companies struggle to build cybersecurity departments from scratch, hindered by the limited number of qualified experts, especially in areas such as incident response, threat identification, and system security testing. An additional challenge is the shortage of mid-level technicians and specialists, which indicates the need to expand training opportunities beyond traditional higher education institutions.

The current education system does not keep pace with the industry's growing needs, necessitating a diversified approach to skills development, including vocational training and practical programs. The lack of such initiatives results in delays in preparing specialists to work in the dynamic and demanding field of cybersecurity.

RECOMMENDATIONS

1. Regular identification of key competency areas in cybersecurity is essential. This should be based on collaboration with the private sector, educational institutions, and industry experts to address both current needs and emerging technological trends.

2. Effective measurement of the skills gap should involve analyzing current and future demand for roles, competencies, skills, and knowledge in cybersecurity, as well as the existing supply of educational and training programs in this area. Society should be made more aware of the current and projected number of cybersecurity specialists and the unfilled vacancies in this field.

3. Research and reporting on the identification of key competency areas should be systematic to continuously monitor digital skills gaps and effectively respond to emerging challenges and the dynamically changing needs of the labor market.

4. It is recommended to establish a central information hub within the activities of existing institutions at the national level (e.g., NCC) and/or EU level (e.g., ENISA). This hub would provide information on the latest cybersecurity trends and expert advice on effective ways to respond to them. Strengthening the visibility of actions taken by these institutions at the national level is also crucial, ensuring that experts and society receive comprehensive information on market conditions in terms of employment opportunities.

5. Employers should actively and regularly communicate their staffing needs and engage in collaboration with universities, schools, and other educational institutions. Joint development and updates of curricula will help tailor education to the dynamically changing demands of the labor market. Reporting on such activities will facilitate more effective management and optimization of educational processes.

6. Providing funding to NGOs will enable them to develop training programs for specialists and employees in cybersecurity. This will increase access to reliable practical courses and certifications, helping to address staffing shortages in the sector.

7. The public sector should intensify collaboration with businesses and educational institutions to improve the quality of education, particularly at the school level. These partnerships can support the implementation of modern teaching methods for computer science and cybersecurity and allow for the dynamic adjustment of training content to the needs of the digital economy.

8. Expanding access to entry-level positions and creating internships and apprenticeships focused on gaining practical experience can activate underrepresented groups in the industry, such as women, individuals with disabilities, and immigrants. These programs should be more flexible to accommodate individuals with varying commitments.

TOPIC III:

Cybersecurity training

Cybersecurity training is becoming increasingly important, but its current state reveals significant challenges. The lack of appropriate digital education from early stages of schooling results in low societal awareness and limited skills for safe navigation in cyberspace. Additionally, traditional teaching methods fail to keep pace with the rapidly evolving digital world, leading to a skills gap. The issue is further exacerbated by limited access to training in less developed regions and widespread resistance to digital education, which hinders society's preparedness for the challenges of modern technology.

CHALLENGES AND RECOMMENDATIONS

CHALLENGES

The lack of adequate curricula and significant gaps in education are major obstacles to building essential digital competencies in society. Fundamental deficiencies stem from improper teaching methods—youth often fail to understand the basic principles of cyberspace, resulting in low awareness of safe behavior in digital environments. The insufficient introduction of digital education in early stages of schooling leads to difficulties in adapting to the technology-driven modern world.

Moreover, resistance to adopting modern teaching methods exacerbates challenges in engaging younger generations and motivating them to expand their knowledge independently. Traditional approaches, based on theoretical knowledge transfer, do not meet the expectations of youth, who prefer interactive and practical forms of learning. Furthermore, limited access to specialized training in less developed regions deepens inequalities in digital skills, hindering professional development and competitiveness in the job market.

Designing effective educational programs in cybersecurity is becoming increasingly challenging due to the dynamic advancement of technology. The pace of digitalization surpasses the development of organized expert knowledge, requiring rapid adaptation in the education sector. Creating effective programs necessitates accounting for the evolving nature of the industry and fostering collaboration across various sectors. Only in this way can educational content be aligned with real market needs and meet the demands of the modern digital economy.

RECOMMENDATIONS

1. Begin Internet safety education in primary schools, teaching children to recognize misinformation and think critically online, explaining that not everything they encounter on the Internet or social media is true. A unified minimum curriculum should be developed to ensure everyone has basic knowledge of safe cyberspace use and understands how to practically utilize modern digital technologies.

2. Cybersecurity training programs must be flexible and designed for regular updates to reflect the dynamic changes in digital threats and tools. These programs should be developed in collaboration with

industry experts and the private sector to deliver the most current knowledge in an accessible manner. It is important that these courses are widely available and, whenever possible, free of charge.

3. Educational materials must be adapted to various social groups, using simple language and intuitive tools to enable both beginners and advanced technology users to acquire knowledge and eliminate entry barriers.

4. Introduce intergenerational workshops that raise awareness about misinformation and online safety. These initiatives can effectively support education while also strengthening social bonds.

5. To address resistance to digital education, modern educational methods that engage and interest participants must be utilized. Educational games that combine entertainment with learning can help develop specific skills and impart knowledge in realistic, interactive contexts. Gamifying educational paths will make the learning process more engaging, motivating, and accessible to a broad audience.

6. Threat scenario simulations, enriched with practical exercises and realistic examples, can significantly enhance the effectiveness of training programs, preparing participants to handle real-world challenges in cyberspace. Students should have the opportunity to address actual cybersecurity issues, such as managing cyber incidents or analyzing misinformation. These exercises develop both technical competencies and collaboration and analytical thinking skills.

7. Practical, interactive activities like workshops and labs are essential to effectively engage youth and enable experiential learning.

8. Highlight the importance of soft skills, including legal, political, and ethical considerations, to clearly show that online safety is not only about technical issues but also about social responsibility awareness.

9. Develop interactive platforms offering courses and innovative tools to address digital skills gaps and prepare younger generations for the challenges of the modern digital reality.

10. Companies and institutions should actively support digital education by co-developing training programs and promoting the idea of responsible digital citizenship. It is crucial to cultivate the concept of an „E-Citizen" capable of functioning in an increasingly digitalized reality.

TOPIC IV:

Cyber hygiene practices and current challenges

Cyber hygiene, defined as a set of practices aimed at the safe use of digital technologies, is becoming an essential part of modern life. The rapid development of technology and increasing threats in cyberspace highlight the lack of sufficient knowledge regarding basic digital safety among both employees and the general public. This issue is exacerbated by a lack of legal regulations, inadequate training approaches, and insufficient cross-sector collaboration. The COVID-19 pandemic and the adoption of remote work systems have significantly exposed these shortcomings, increasing the vulnerability of organizations and users to cyber threats. In an increasingly digital world, the development and implementation of effective cyber hygiene practices are crucial to ensuring security at both individual and organizational levels.

CHALLENGES AND RECOMMENDATIONS

CHALLENGES

The state plays a key role in promoting and enforcing cyber hygiene principles, as it can introduce regulations that make these practices an integral part of daily life. The absence of such regulations means cyber hygiene is not prioritized, leading to a lower level of societal cyber resilience. The approach to cyber hygiene training needs to change, emphasizing intensified cross-sector collaboration. Such collaboration helps experts and trainers tailor programs to new threats and market demands. Failure to align training with technological developments can leave society unprepared for emerging threats. A lack of updates to training content may also reduce interest, lowering their effectiveness. Evaluating the effectiveness of training is essential and allows for the necessary modifications to support the development of cyber hygiene.

Educational initiatives can support the growth of cyber hygiene by enabling access to training. Examples include the Global Cyber Alliance (GCA), which developed cybersecurity toolkits to eliminate financial barriers and provide basic protection tools for small and medium-sized businesses, non-profits, and individual users. Another notable initiative is Cyberpeace Builders by the Cyberpeace Institute, which addresses skill gaps in technical assistance by offering technological support to vulnerable organizations such as hospitals and humanitarian groups.

The COVID-19 pandemic has transformed work models, forcing organizations worldwide to rapidly adapt to remote work systems. A significant portion of employees began working outside the office. While this model has brought many benefits to individuals, it has also introduced new challenges related to digital security. There is a notable shortage of basic knowledge about digital safety and practical skills, such as understanding data structures or principles for securely sharing information.

RECOMMENDATIONS

1. Efforts should be made to increase awareness of available cyber hygiene training and facilitate access to it. Digital tools such as the M-Obywatel application can serve as effective communication channels, remin-

ding users about training sessions, events, and educational resources. Information campaigns should emphasize the benefits of enhancing digital security skills.

2. Cyber hygiene practices should be codified into law and implemented as a standard for entities within the National Cybersecurity System (KSC). Regulations requiring regular digital security training for critical sectors of the economy are essential.

3. Cyber hygiene training should be easily accessible, free of charge, and offered at various levels of advancement—from basic courses for beginners to advanced programs for IT specialists. Digital solutions such as e-learning platforms, mobile applications, and informational portals can significantly increase access to education, supporting the development of cybersecurity skills across a broad social spectrum.

4. Cyber hygiene education should be conducted systematically and constantly adapted to new challenges and evolving digital threats. Educational content must be regularly reviewed and updated to ensure its relevance. This approach not only increases societal awareness but also contributes to building resilience against increasingly common cyber threats.

5. An integrated approach that includes educational programs in schools and simplified tools and practices for end-users is needed. Employers should be legally required to organize training that incorporates cyber hygiene and digital safety practices. This will enhance organizational resilience to cyber threats and mitigate undesirable legal and financial consequences, such as data loss or server attacks. Non-governmental organizations specializing in cybersecurity can play a crucial role in creating materials tailored to the specific needs of different target groups. Such training should be brief but conducted periodically to facilitate knowledge retention.

6. Implement mechanisms to assess the effectiveness of educational initiatives in the field of cyber hygiene. Analyzing results will enable improvements in training programs, enhancing their efficiency.

7. States and organizations should establish standard digital safety principles and digital workplace safety and hygiene guidelines, including both universal directives and detailed recommendations for specific roles. Mandatory training and tests based on practical examples should be conducted annually. Experience from institutions such as The Polish Cyber Command shows that such measures can improve organizational resilience by up to 30%.

TOPIC V:

Cross-sectoral cooperation

Cross-sectoral cooperation plays a key role in building resilience to cyber threats and developing competencies essential in the digital world. The rapid pace of technological advancement requires the engagement of the public, private, educational sectors, and non-governmental organizations, to create coherent strategies and programs that meet current market needs. Public-private partnerships and collaboration with local governments allow for better resource utilization, support innovative educational and training initiatives, and help close the skills gap in society. Effective partnerships not only enhance cybersecurity levels but also support the development of local communities and their ability to adapt to rapidly changing digital challenges.

CHALLENGES AND RECOMMENDATIONS

CHALLENGES

Building a resilient society requires the involvement of both the public and private sectors in developing coherent strategies for skills development. Public-private partnerships (PPPs) have proven to be an effective model of such collaboration, which can be used to increase the efficiency of training programs and play a vital role in skills development. Collaboration among various stakeholders enables better resource utilization and the identification of specific cybersecurity needs. These partnerships facilitate the implementation of innovative initiatives, such as intergenerational workshops or specialized programs for different social groups, supporting the development of competencies to address the rapidly changing technological environment.

Educational institutions, as knowledge leaders, can leverage international research and trends to design curricula aligned with current labor market requirements. At the same time, close collaboration between educational institutions and industry enables the anticipation of needs and the adaptation of training programs. Such partnerships can play a crucial role in creating effective cybersecurity training programs, especially by engaging various social groups and institutions at all levels. Industry, educational institutions, and public institutions play key, complementary roles in identifying and addressing specific cybersecurity skills needs. Private companies also serve an informational role by providing data on market and technological needs, allowing for the continuous adaptation of curricula. Internships and apprenticeships organized by companies help verify acquired competencies, identify gaps that need to be addressed, and support certifications and internal training. Collaboration with local governments, which can promote cybersecurity education, is also a significant step in closing the skills gap in society. This will enable effective adaptation to the challenges of the modern world.

RECOMMENDATIONS

1. Introduce platforms that enable companies to provide feedback to academic centers and educational institutions on curricula, allowing the continuous adaptation of educational offerings to labor market requirements. Supporting feedback loops with indu-

stry is essential to ensure that cybersecurity training programs reflect the latest threats and technical requirements. Formal mechanisms for industry feedback, such as including private sector representatives in advisory boards of educational institutions, should be implemented.

2. Enterprises should actively define their current and future needs, support the development of their employees' skills, and promote flexible educational models that include both technical and interpersonal skills. Regular consultations on graduate expectations and curriculum updates are fundamental to aligning education with real-world challenges.

3. Public-private partnerships (PPPs) should focus on impact and addressing skills needs with measurable indicators. Foundations, NGOs, and state institutions can jointly conduct educational and training programs tailored to the needs of various groups, such as seniors, children, and individuals with low digital skills.

4. Create a cohesive education system that enables continuous knowledge and skills updates, considering the rapid pace of technological development. Priority should be given to introducing curricula that foster critical thinking, data analysis, and risk assessment.

5. PPPs can support the development of local cybersecurity initiatives and structures, particularly through collaboration with local governments. Such actions will help develop competencies in underprivileged regions often overlooked in central educational strategies, making programs more flexible, accessible, and aligned with the latest technological trends.

6. The state should provide strategic support by financing educational initiatives and creating regulations that facilitate cross-sectoral cooperation. Governments can influence local authorities to require the establishment of cybersecurity structures and support local educational programs. These actions ensure a common language and understanding among stakeholders, leveraging frameworks and standards.

7. Local governments can initiate local educational programs, organize intergenerational workshops, and engage various social groups in activities.

8. Educational grants, municipal funds, or EU funding can significantly contribute to implementing training projects. Simplifying application procedures and reducing bureaucracy will increase the efficiency of using available resources.

9. Coordinated initiatives supporting the implementation of digital competency development tasks, such as those of ECCC or ENISA at the EU national levels, are essential. The Ministry of Digital Affairs should consider establishing a coordinated network of 16 information-educational centers at the regional level. Their tasks would include informational campaigns, educational campaigns for primary and secondary school students, seniors, and local communities, as well as specialized training for higher education institutions. These centers would also collaborate with local governments to develop and implement cybersecurity sector strategies. Such centers could serve an informational role for the Ministry while implementing continuous and systematic actions to enhance digital competencies, including cybersecurity and misinformation identification. Annual evaluative consultations with private sector representatives would allow for curriculum adaptation and systemic inclusion of digital education in the teaching process. Implementing similar solutions nationally in EU member states will contribute to effectively establishing and directly implementing unified digital competency standards.

10. Companies should actively offer entry-level positions to individuals new to the job market, enabling skill development and addressing the industry's demand for a qualified workforce.

11. Partnerships should be based on measurable goals that account for flexibility and adaptability to new challenges. As the technological landscape evolves, strategies and long-term objectives should be regularly updated.

12. To ensure the sustainability of multi-stakeholder training initiatives, it is essential to document experiences and outcomes, enabling better management of educational processes and their adaptation to changing requirements. Implementing modular programs that can be modified according to emerging technologies and threats will ensure greater relevance and effectiveness.

Summary of key recommendations

The key recommendations are summarized below, organized by priority for action:

1. Challenges in cyber security:

- Creating a catalog of digital competencies with both soft and hard skills.
- Early education in critical thinking and digital health and safety.

2. Competency gap mapping:

- Regular identification of competency gaps with private sector participation.
- Creating central information points to support the labor market and education.

3. Training in cyber security:

- Flexible, practical and regularly updated training programs.
- Introducing educational games and simulated threat scenarios.

4. Cyber hygiene practices:

- Incorporating cyberhygiene standards into regulations and mandatory employee training.
- Creating intuitive educational tools and applications.

5. Cross-sector cooperation:

- Strengthening cooperation between PPPs and with local governments on local education programs.
- Developing information and education networks at regional and national levels.

Deloitte.

Challenges of the NIS2 Directive

The NIS2 Directive, which aims to increase the level of security of network and information systems in the European Union, poses new challenges for organizations. These include both the adaptation of existing processes and the implementation of new technical, legal and organizational solutions. Failure to comply with the requirements may result in high financial penalties and damage to the company's reputation. Therefore, it is worth taking action now to ensure compliance with the new regulations.

Key challenges of the NIS2 Directive

1. Security Gap Analysis: Organizations must conduct a comprehensive assessment of current systems and processes to identify areas for improvement.

2. Implementation of new requirements: The implementation of technical safeguards, such as threat detection systems or incident management, requires time, resources and appropriate know-how.

3. Legal compliance: The directive imposes the obligation to meet certain formal requirements, such as incident reporting or risk management.

4. Maintaining Compliance: Organizations must constantly monitor their systems and adapt procedures to changing legal and technological requirements.

How can Deloitte help?

Deloitte specializes in comprehensive support for organizations in the process of meeting the requirements of the NIS2 directive. Our services include:

1. Gap analysis:

- We conduct detailed audits, identifying areas where the organization does not meet NIS2 requirements.
- We prepare a report with recommendations, indicating specific steps to take.

2. Requirements Implementation:

- We help you implement appropriate technical measures, such as information security management systems (ISMS), and processes in accordance with best practices.
- We support the development and implementation of business continuity plans and incident response strategies.

3. Legal and organizational consulting:

- We cooperate with legal experts to ensure full formal and legal compliance.
- We advise on risk management and creating a safety culture in the organization.

4. Maintaining Compliance:

- We offer monitoring, training and process update services to ensure long-term compliance with the Directive.

Why is it worth acting now?

The NIS2 directive imposes strict deadlines for implementing the requirements, and the process of adapting the organization is time-consuming. Starting action now allows you to avoid rushing, minimize the risk of fines, and build a solid foundation for digital security.

Take action today! Contact Deloitte for a free consultation and to find out how we can help your organization meet the requirements of the NIS2 directive.