Co-funded by the European Union

D6.3 POLICY RECOMMENDATIONS

CYBER AGENT 06.2026

Call: ERASMUS-EDU-2022-PI-ALL-INNO
Type of Action: ERASMUS-LS
Project No. 101111732

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

www.cyberagents.eu

Work Package 6: Dissemination & Exploitation

Deliverable D6.3: Policy Recommendations

Leader of WP6 – Women4Cyber Foundation

CONTENT

LIST OF TABLES

INTRODUCTION

SMEs make up more than 90% of businesses across Europe, yet they are among the most exposed to cyber threats and among the least equipped to deal with them. The gap between the scale of the risk and the capacity of most SMEs to respond to it is not primarily a technology problem. It is a people and skills problem.

The CyberAgent Project was built around the premise that every SME has the potential to develop in-house cybersecurity expertise and improve its cybersecurity practices, provided its employees have access to flexible and accessible training. The project brought together higher education institutions, vocational training providers, and SMEs from eight European countries to develop a structured programme for training SME employees as Cyber Security Change Agents. This role is conceived to ensure and drive lasting improvements in cybersecurity practices from within their organisations.

Over three years, the consortium developed and piloted a learning pathway covering technical skills, analytical thinking, risk management, and organisational competences. The curriculum was designed from the outset to be modular, portable, and usable in university settings, vocational training, and workplaces. Moreover, the curriculum is aligned with European qualification frameworks to ensure that what participants learn is fully recognised.

The pilot training programme welcomed 594 participants from Belgium, Norway, Türkiye, Finland, Poland, Spain, Romania, and Lithuania. The distribution of the participants to the programme exceeded the project indicators and reached all target groups: HEI students, HEI trainers, VET students, VET trainers, and SME employees. The dissemination of the CyberAgent pilot reached 354 male participants, 226 female participants, and 14 participants who preferred not to disclose their gender. The broad and diverse audience shows that the content of the pilot training programme reached learners who already form part of the workforce and that the format used is flexible enough for professionals to participate and balance the programme with their professional commitments.

1. SCOPE AND METHODOLOGY

1.1. PURPOSE OF THE DELIVERABLE

This deliverable examines how the CyberAgent project's work relates to existing EU policies on cybersecurity, skills, and gender equality, and sets out recommendations for improvements in these areas. It is addressed to policymakers, educational institutions, and industry stakeholders with a role in shaping how cybersecurity upskilling is designed and recognised across the EU. In particular, it is addressed to the entities that can make a difference in the upskilling and lifelong learning of the European SMEs workforce and underrepresented groups in the cybersecurity field such as women. Drawing on three years of research and piloting activity carried out across eight European countries, the document pursues three practical aims:

- It highlights how the CyberAgent project contributes to enhancing SMEs cyber resilience and building a sustainable cybersecurity culture within organisations that lack dedicated security resources and, at the same time, are the most exposed to threats.
- It identifies the structural challenges observed in policy frameworks, training systems, and participation patterns that limit the effectiveness and reach of cybersecurity upskilling.
- It provides recommendations for future EU policies on engagement with SMEs in the cybersecurity ecosystem, on the integration of cybersecurity competences into VET and HEI systems, and on the gender dimension of cybersecurity workforce development.

The document is intended to be read as a contribution to the broader policy conversation about how Europe builds cyber resilience from the ground up, starting with the people who work in its smallest and most exposed organisations.

1.2. METHODOLOGICAL APPROACH

The methodological approach of this report draws on the evidence, both qualitative and quantitative, collected throughout all phases of the CyberAgent project. Sources include cybersecurity policies and regulations at EU level, previously published deliverables such as the Training Needs Mapping Report (D2.2), which surveyed 190 VET and HEI educators and 176 SME representatives across partner countries, the national piloting reports submitted by eight partner organisations following their respective pilot implementations, and pilot analytics covering 594 registered users.

The purpose of this deliverable is not to provide an exhaustive mapping of all relevant EU legislation or regulatory frameworks concerning cybersecurity, digital skills, and SME resilience. Instead, the report selectively engages with the policy areas where the CyberAgent project can generate concrete insights, specifically: SME cyber resilience and the human factors that shape it; cybersecurity skills development and lifelong learning within VET, HEI, and workplace contexts; gender balance and inclusion in the IT and cybersecurity sector.

The recommendations presented in this document are derived directly from project findings, (like The SME Cyber Security Change Agents Training needs mapping report (D2.2), Training Program Evaluation (D5.3)), validated quantitative indicators (KPIs), and target group impact assessment questionnaires, ensuring full alignment with the project's Quality Assurance and Monitoring Plan (D1.3), and are intended to be actionable and oriented toward specific decisions that policymakers, SMEs, and educational institutions can make, rather than general observations about the importance of cybersecurity or the existence of a skills and gender gap.

In addition to the project's evidence base, the report draws on perspectives gathered from senior figures in the European cybersecurity and industry community. Representatives from Women4Cyber, the Belgian Cyber Security Coalition, and the European Cyber Security Organisation (ECSO) were consulted to validate the project's findings against broader industry experience and to ensure that the recommendations reflect not only the consortium's implementation perspective but the wider professional and policy landscape in which SMEs cybersecurity upskilling takes place. Their insights are presented directly in the Key Project Outputs section.

2. STATE OF THE ART

Cybersecurity has rapidly ascended to the top of the EU's digital policy agenda, becoming a key area of the European Union's broader digitale transformation efforts. As cyber threats grow in scale and societal impact, the EU intensified its focus on building a resilient digital ecosystem capable of protecting citizens, businesses, and public institutions at EU and national level. Within this evolving landscape, three intersecting EU policy streams stand out as particularly relevant to the CyberAgent Project: the regulatory framework for cybersecurity, the education and skills agenda, and the gender dimension of the digital workforce.

These three policy streams are not isolated or distant from each other. The increasing cybersecurity regulations demand for more skilled professionals to take over technical and non-technical roles, while the constant underrepresentation of women in cybersecurity and the broader ICT sector limits the talent pool available to meet this demand. At the same time, EU-level initiatives on digital skills and inclusion aim to ensure that the benefits of the digital transition are shared broadly across society, including among women.

This section will therefore gather and contextualise the strategies and regulatory instruments across these three domains that are most relevant to the CyberAgent project, outlining the broader EU policy environment in which the project operates and to which it contributes.

2.1. CYBERSECURITY REGULATIONS

This subsection maps the key EU regulatory instruments that define the cybersecurity obligations and expectations within which the CyberAgent project operates. Rather than providing a comprehensive mapping of all existing regulations, it focuses on the points of direct relevance to the project's core objectives.

2.1.1. NIS2 DIRECTIVE (EU 2022/2555)

The Network and Information Security 2 Directive (EU 2022/2555), adopted in December 2022 and entered into force in January 2023, became enforceable across Member States starting from October 2024. The NIS2 Directive represents the most significant expansion of cybersecurity obligations to date. It broadens the scope of mandatory risk management and incdent reporting to cover SMEs across 18 critical sectors, including manufacturing, health, transport, and digital infrastructure. Crucially, it introduces explicit accountability of top management for cybersecurity failures. This shift elevates cybersecurity from a technical domain to an organisational culture issue.

NIS2 requires organisations across sectors to adopt risk management measures, ensure continuous staff training and cybersecurity hygiene practices, and promote awareness at all organisational levels. This directly aligns with the CyberAgent training's focus on building cybersecurity competence among SME employees who are often the first line of defence against increasing cyber threats. Moreover, the CyberAgent training modules, particularly M1 (Security Programme Management), M5 (Security Governance and Policy), and M7 (Risk Management), directly support the competence baseline that NIS2 expects organisations and their staff to promote and maintain.

2.1.2. GENERAL DATA PROTECTION REGULATION (REGULATION (EU) 2016/679)

The General Data Protection Regulation (GDPR) is the foundational framework at EU level governing the protection of personal data and remains tightly linked to cybersecurity obligations. The GDPR Regulation requires organisations to implement appropriate technical and organisational measures to ensure a risk-appropriate level of security. This includes measures to ensure confidentiality and integrity of processing systems. For SMEs, compliance with GDPR security obligations requires a basic level of cybersecurity literacy that goes beyond technical staff. Employees in roles such as HR, administration, and sales often handle personal data and must therefore understand data protection principles, recognise risks such as phishing and social engineering, and the procedures to report incidents.

This is precisely the audience and the skill level that the CyberAgent pilot targeted in modules such as M1 (Security Programme Management), M3 (Analytical Tools), and M8 (Business Continuity). These parts of the pilot support the organisational security culture that GDPR compliance in SMEs heavily depends on.

2.1.3. CYBER RESILIENCE ACT (REGULATION (EU) 2024/2847)

The Cyber Resilience Act (CRA), adopted in 2024, further extends security-by-design obligations by introducing binding horizontal cybersecurity requirements for all products with digital elements placed on the EU market. It marks a significant shift from the previous *modus operandi*, introducing enforceable obligations across the product lifecycle. While the primary obligations fall on manufacturers and importers, the supply chain implications of this regulation also fall directly on the SMEs that resell or maintain digital products as part of their businesses.

This represents an important change in the compliance landscape for SMEs. By placing obligations on the product itself, the CRA reflects a broader EU policy shift towards treating cybersecurity as a shared responsibility within organisations, not only as the domain of large technology companies. For employees working for SMEs that develop digital products or operate within digital supply chains, understanding cybersecurity requirements (such as vulnerability management, incident reporting, and secure-by-design principles) is a clear business imperative.

The CyberAgent modules M4 (Security Operations), M5 (Security Governance and Policy) and M7 (Risk Management) bring direct value to this framework by equipping non-technical employees with the conceptual foundations needed to understand the compliance structure required by the CRA. The project's impact is particularly relevant in this context, as SMEs that lack dedicated compliance or cybersecurity staff could highly benefit from a Cybersecurity Change Agent, an internal advocate who can embed security and compliance in day-to-day operational practice.

2.1.4. EU CYBERSECURITY STRATEGY (2020) AND THE EUROPEAN CYBERSECURITY SKILLS FRAMEWORK (ECSF)

The EU Cybersecurity Strategy of 2020 framed the EU's ambition to build cyber resilience, develop cybersecurity capabilities, and foster the development of a skilled cybersecurity workforce. One of its anchors explicitly mentions the need to address the cybersecurity skills gap, particularly by making cybersecurity education more accessible and inclusive, and by targeting non-technical employees instead of only involving specialised professionals.

The European Cybersecurity Skills Framework (ECSF), published by ENISA in 2022, provides a reference framework for cybersecurity pathways and competences. While the ECSF primarily targets specialised and technical roles, it provides a useful backdrop for understanding the continuous skills development that the CyberAgent project addresses at its foundation. The CyberAgent pilot training is positioned as an inclusive awareness and upskilling training programme for non-expert audiences, covering the baseline competences that sit below and feed into the roles defined by the ECSF such as cybersecurity implementer, cybersecurity risk manager, and cybersecurity educator.

Table 2. Summary of relevant cybersecurity policy and regulations

Policy	Relevance to CyberAgent	CyberAgent training modules
NIS2 Directive (2022/2555)	Staff training and cybersecurity hygiene practices for SMEs	M1, M5, M7
GDPR (2016/679)	Security measures and data protection awareness for all staff handling personal data	M1, M3, M8
Cyber Resilience Act (2024/2847)	SME obligations in digital product and supply chain security	M2, M4, M5
EU Cybersecurity Strategy 2020 / ECSF Framework	Skills gap rationale; foundational competence framework	All modules

2.2. EDUCATION AND SKILLS

At the VET level, national landscapes across partner countries (Lithuania, Belgium, Norway, Finland, Poland, Romania, Spain, Turkey) reveal a consistent pattern: cybersecurity is rarely a standalone subject in VET curricula but, instead, it's fragmented across a series of broader IT modules, leaving significant gaps in structured, competence-based training for non-IT professionals. The CyberAgent Training Needs Mapping Report (D2.2) confirmed this finding through surveys that involved 190 VET/HEI educators and 176 SMEs representatives across partner countries.

This evidence raises a key issue about cybersecurity upskilling for existing SME employees: those without an IT background are systematically underserved by current HEI and VET offerings across partner countries. Existing programmes are largely designed for students entering the field and in need of a broader perspective, not for accountants, HR managers or administrative staff who need to understand and act on cybersecurity risks as part of their everyday work, especially if they handle personal data. Closing this gap requires a reorientation of training away from purely technical curricula and toward cybersecurity risk-management competences that can be applied by non-technical employees, transforming them into Cybersecurity Change Agents.

2.2.1. EUROPEAN QUALIFICATIONS FRAMEWORK (EQF – RECOMMENDATION 2017/C189/03)

The EQF provides the main reference framework for comparing qualifications across EU Member States by anchoring them to eight levels defined by learning outcomes: knowledge, skills, and competences. The CyberAgent pilot's modules are aligned to EQF levels 4-6, making the programme legible across national qualification systems and accessible to both VET and HEI learners. This alignment is particularly significant for SME employees who may lack formal cybersecurity qualifications but hold professional experience: the approach of the EQF allows competence gains to be recognised independently of the route through which they were acquired, academic or professional.

The 2017 Recommendation also encourages Member States to link national qualifications frameworks to the EQF and to support the validation of non-formal and informal learning. This principle is directly relevant to CyberAgent's workplace-based delivery model, where SME employees acquire competences outside formal educational settings.

2.2.2. DIGITAL EDUCATION ACTION PLAN (2021-2027)

The Digital Education Action Plan (DEAP) sets out the EU's strategic vision for digital transformation in education and training across two priority areas: fostering the development of a high-performing digital education ecosystem and improving digital skills and competences for the digital transformation. The DEAP specifically targets the improvement of digital competences at all levels of education, including the integration of cybersecurity awareness into curricula across VET and HEI. It also supports flexible, modular, and short-cycle learning formats as a mean of reaching learners who cannot access or complete traditional qualification pathways. This design logic is clearly reflected in CyberAgent's self-paced, online, module-by-module delivery. The emphasis on reaching underrepresented audiences and those with low prior digital competence further aligns with the project's explicit targeting of non-IT professionals in SME environments.

Table 2. Summary of relevant education and skills regulations

Policy	Relevance to CyberAgent
EQF Recommendation (2017)	Qualifications architecture; learning-outcomes recognition; validation of non-formal learning
Digital Education Action Plan (2021–2027)	Cybersecurity in curricula; flexible and short-cycle upskilling formats

2.3. GENDER DIMENSION

The underrepresentation of women in cybersecurity is a well-documented and persistent structural challenge across the EU. According to ISC2, women currently represent approximately 20% of the cybersecurity workforce in Europe, a figure that has remained stagnant in the past decade. The pipeline problem begins early: women are significantly underrepresented in ICT-related VET and HEI programmes, and the gap increases across career stages. For SMEs specifically, this means that the talent pool is male-dominated, and that women in non-IT roles within SMEs are among the least likely to receive targeted cybersecurity training.

The CyberAgent pilot data reflects the broader landscape but also demonstrates meaningful progress. Of the 594 platform users recorded during the piloting phase, 226 were women, representing approximately 38% of registered participants. While male participants formed the largest group, which is consistent with patterns in cybersecurity-related training, the share of women reached through CyberAgent is notably higher than the sector average in Europe (22% as per a 2025 ISC2 survey) and reflects the deliberate outreach strategies deployed by partners, including Women4Cyber Foundation in Belgium, women-focused professional networks in other partner countries, and education-based recruitment channels that reach more gender-balanced audiences.

In particular, the Women4Cyber Foundation, a CyberAgent project consortium partner and Belgian pilot lead, was established to promote the inclusion of women in cybersecurity across Europe. Its involvement in CyberAgent reflects a deliberate project design choice to embed gender inclusion expertise directly into the consortium. The Foundation's recruitment approach for the Belgian pilot, which generated over 800 expressions of interest across Europe through targeted outreach and resulted in a participant group that was 89% women, demonstrates the impact of gender-focused recruitment strategies when applied with dedicated expertise and network reach.

2.3.1. GENDER PARTICIPATION ACROSS PARTNER COUNTRIES

The gender distribution across national pilots, documented in the CyberAgent Pilot Evaluation Report (D5.3), reveals significant variation between partner countries, both in the proportion of women reached and in the profile of female participants across target groups.[1]

Belgium: of the 66 selected participants, 40 were women and only 25 were men. This outcome was directly linked to the recruitment strategy led by Women4Cyber Foundation, which used targeted outreach through CyberAgent and Women4Cyber social media channels and a dedicated LinkedIn form, generating over 800 expressions of interest before eligibility screening reduced the group to 66 participants.

[1] The data was extracted from Table 5 of D5.3 “CyberAgent Upskilling Training Programme”

Lithuania: 49 women registered out of 136 total participants. Of these, 42 women passed at least one module, compared to 63 men out of 79 registered male participants. Women in Lithuania not only participated in significant numbers but also showed strong completion rates relative to their registration numbers.

Poland: 34 women among 79 registered participants, alongside 44 men and 1 undisclosed.

Romania: among SME participants, 7 were women and only 2 were men. However, among HEI participants, the distribution was reversed, with 11 women and 18 men.

Norway: recorded 14 women and 28 men across all target groups.

Finland: reached 12 women and 22 men among its 34 registered participants. The Finnish pilot was smaller in scale, with recruitment focused on motivated learners through targeted outreach rather than open calls.

Spain: reported that approximately 29.3% of overall participants were women and 68.5% were men.

Türkiye: recorded the largest gender imbalance of all partner countries, with women representing approximately 19% of participants and men 80%.

Taken together, these figures validate two critical structural insights for future European skills policy. First, the gender gap in cybersecurity training participation remains deeply entrenched across the European digital landscape, as evidenced by the baseline data across seven partner countries where female representation was significantly diversified. However, the exceptional outcome in Belgium, proves that this gap is not immutable but can be radically corrected through deliberate, network-based, gender-sensitive outreach structures rather than passive open calls. Second, the pilot data confirms that these skills and participation gap is acutely concentrated at the SME level, which constitutes the primary target group of the CyberAgent framework. Because SME workforce learners demonstrate a strict pedagogical preference for compact, governance-oriented training rather than extensive technical pathways due to severe time constraints, these regional and sectoral disparities cannot be solved by traditional educational offerings. Consequently, these findings establish a definitive policy mandate for the European Commission and Member States to structurally support and fund short-cycle, flexible micro-credential models tailored to specific workforce profiles, ensuring that cybersecurity literacy is recognized as a foundational digital competence across all levels of the EU economy.

2.3.2. EU GENDER EQUALITY STRATEGY (2020-2025)

The EU Gender Equality Strategy 2020 - 2025 sets out the European Commission's framework for achieving gender equality across economic, social, and institutional domains. Among its key objectives is closing gender gaps in the labour market, including in digital and technology sectors where women remain significantly underrepresented. The Strategy explicitly calls for targeted measures to increase women's participation in the STEM and ICT fields, and links gender equality in the digital economy to the broader goals of economic resilience and competitiveness for the European Union.

The Strategy moves beyond symbolic commitments by calling for structural interventions in education, hiring practices, and company culture that address the root causes of underrepresentation rather than its symptoms. It recognises that the digital transition, if left unmanaged, risks deepening existing gender inequalities by concentrating the economic gains of digitalisation in sectors or roles where women are already a minority. As mentioned above, cybersecurity is a concrete example of this dynamic: it is one of the fastest growing fields, yet women remain marginalised in both its workforce and its training pipelines. For CyberAgent, the Gender Equality Strategy provides the foundational policy rationale for treating women's participation as a core design and evaluation criterion of the project.

3. KEY PROJECT OUTPUTS

The CyberAgent project produced a set of interrelated outputs spanning curriculum development, training delivery, needs analysis, and implementation guidance. Each output responds to a specific gap identified in the policy landscape mapped in the sections above, and together they constitute a coherent upskilling infrastructure for cybersecurity awareness in SMEs, VET, and HEI contexts.

3.1. TRAINING NEEDS MAPPING REPORT (D2.2)

The Training Needs Mapping Report is the project's foundational analytical output, produced through surveys involving 190 VET and HEI educators and 176 SME representatives across the eight partner countries. It documents the state of cybersecurity education provision at national level, identified competence gaps among non-IT professionals in SME environments, and established the evidence base for the curriculum design of the CyberAgent training pilot.

From a policy perspective, this output directly responds to the objectives of the Digital Education Action Plan and the European Skills Agenda, both of which call for evidence-based identification of skills gaps as a precondition for the development of effective upskilling and training initiatives. The report's consistent finding that cybersecurity is fragmented across VET curricula and largely absent as a standalone competence for non-IT SME employees, validates the project's intervention logic and provides a needs-assessment methodology that could be replicated by other initiatives.

3.2. CYBERAGENT TRAINING PLATFORM AND MODULES

The core output of the project is the CyberAgent online learning platform and its nine training modules, designed and aligned to EQF levels 4-6. The modules cover Security Program Management (M1), System Administration (M2), Analytical Tools (M3), Security Operations (M4), Security Governance and Policy (M5), Cybersecurity Planning (M6), Risk Management and Mitigation (M7), Business Continuity (M8) and Empowering Cybersecurity Careers (M9).

The curriculum responds directly to multiple policy frameworks. Its EQF alignment meets the requirements of the 2017 EQF Recommendation and positions each module as a building block within national qualification systems. Its modular and self-paced structure enables individual modules to be formalised as stackable micro-credentials by partner institutions. Its coverage of security governance, risk management, and data protection addresses the staff competence expectations embedded in the NIS2 Directive and GDPR Regulation. Its accessibility to non-specialist learners responds to ENISA's calls for entry level and awareness-focused training that reaches the broadest possible segment of the SME workforce.

The piloting phase validated the curriculum at scale. Across eight countries, the platform recorded 2,410 module registrations, 1,547 course starts and 1,060 passed module tests, with 89.3% of survey respondents reporting an increase in their cybersecurity knowledge following participation.

3.3. DIFFERENTIATED IMPLEMENTATION MODELS (HEI, VET, SME)

Based on the evidence gathered during the national pilots, the project confirmed the value of a differentiated implementation approach and set out three recommended models for HEI settings, VET settings, and SME workplace delivery, providing a structured guidance on recruitment, facilitation, learning pathway design, support mechanisms, and follow-up for each context. These models are proposed for adoption in the next phase of the programme.

These models respond to the principle that generic, one-size-fits-all training delivery consistently underperforms when applied to heterogeneous learner populations. The SME implementation model in particular, with its emphasis on flexibility, short practical pathways and workplace relevance, directly operationalises these principles for a target group that standard educational delivery formats routinely fail to reach.

3.4. INDUSTRY AND STAKEHOLDERS' PERSPECTIVES

The design and outcomes of the CyberAgent project have been recognised by senior figures from the EU cybersecurity community. The following perspectives, gathered from key stakeholders in the project's network, reflect a shared conviction that cybersecurity resilience in SME environments is fundamentally a cultural and human challenge, and that projects like CyberAgent, which place non-specialist employees at the centre of the response, represent a necessary and strategic shift in how the field approaches workforce development and resilience.

Elena Santiago Cid — Vice President, Women4Cyber and former Director, CEN-CENELEC

"SMEs are the backbone of the European economy, yet they remain disproportionately exposed to cyber threats without enough resources to defend themselves. The Cyber Agent project recognised that cyber resilience is not purely a technical challenge, it is a cultural one. Empowering women employees to become Cybersecurity Change Agents creates a lasting, scalable line of defense within companies and organisations. At Women4Cyber, we are especially committed to initiatives that place women at the centre of this mission, because diversity in cybersecurity is a strategic imperative for a more resilient digital Europe."

Henk Dujardin — CEO, Belgian Cyber Security Coalition

"*In a threat landscape that is becoming more complex by the day, SMEs need cybersecurity to be lived, not delegated. By empowering Cybersecurity Change Agents, a powerful initiative that turns diversity and inclusion into structural impact, we embed security awareness and resilience where it matters most: within everyday business culture*."

Roberto Cascella — CTO, European Cyber Security Organisation (ECSO)

"*Cybersecurity is not only a technical or operational concern - it must be embedded in culture, workflows, and decision-making. Cybersecurity Change Agents play an essential role in enabling this shift: acting as a bridge between technical experts and the wider organisation and translating risks into operational and strategic priorities that leadership can act upon, and ensuring alignment with business objectives. This is especially critical for SMEs, where such roles can help elevate cybersecurity from a technical issue to a governance imperative*."

The consistency across these three perspectives reinforces the project's central argument: that the Cybersecurity Change Agent is a key role that addresses a gap that is widely recognised at senior levels of the European cybersecurity community but has rarely been tackled through accessible and structured training.

4. RECOMMENDATIONS FOR FUTURE POLICY AND PRACTICE

The evidence gathered through the CyberAgent piloting phase, combined with the EU policy landscape mapped in the previous sections, points to a set of concrete recommendations directed at interconnected audiences: policymakers at EU and national level working on cybersecurity, employers and employees within the SME ecosystem, and policymakers and civil society representatives working to advance gender inclusion in cybersecurity. These recommendations are grounded in the project's implementation experience across eight countries and in the gaps that the pilot data and participants' feedback consistently brought up.

4.1. POLICYMAKERS

This section sets out recommendations directed at policymakers at EU and national level who are responsible for designing and coordinating the regulatory and skills frameworks within which cybersecurity upskilling takes place. The recommendations draw on the CyberAgent training pilot implementation experience to identify specific gaps and opportunities in the current policy landscape where targeted action would significantly strengthen the EU's capacity to build cybersecurity resilience at scale.

4.1.1. RECOGNISE CYBERSECURITY LITERACY AS FOUNDATIONAL DIGITAL COMPETENCE

Current EU policy instruments, including NIS2 and the Cyber Resilience Act, place cybersecurity obligations on organisations without providing a corresponding framework for how non-specialist employees should be supported to meet those obligations. Policymakers should explicitly integrate cybersecurity awareness into the framework of digital competences at foundational and intermediate proficiency levels. This would help embedding cybersecurity literacy in day-to-day work across sectors and would facilitate the integration of the role of the Cybersecurity Change Agent within SMEs.

4.1.2. EMBED THE CYBERAGENT MODEL IN NATIONAL CYBERSECURITY STRATEGIES

The Cybersecurity Change Agent figure is a trained, non-specialist employee who acts as an internal advocate for cybersecurity awareness. This role should be recognised and promoted within national cybersecurity strategies as an effective mechanism for building resilience in organisations that cannot sustain dedicated security staff. Policymakers could support this by developing a national certification or badge system for Cybersecurity Change Agents, aligned to the ECSF, that gives the role visibility and legitimacy within SME organisational cultures across member states.

4.1.3. ENCOURAGE SHORT-CYCLE MICRO-CREDENTIAL MODELS TAILORED TO SPECIFIC LEARNER PROFILES

The CyberAgent evidence base makes a clear case for moving beyond generic training pathways. The Training Needs Mapping Report (D2.2) confirmed that SME employees face severe time constraints that make extended training formats inaccessible. Short-cycle micro-credential pathways are therefore the most appropriate default format for workplace-based cybersecurity upskilling. The CyberAgent platform has already deployed a dedicated microlearning environment that demonstrates the feasibility of this approach. Policymakers should now provide the funding and recognition frameworks that allow differentiated micro-credential models to be adopted at scale across VET and HEI systems across the EU.

4.2. SME ECOSYSTEM

This section addresses the actors who shape the environment in which SMEs operate and learn. The recommendations focus on practical shifts in how cybersecurity culture and upskilling are framed, delivered, and embedded within SME organisational culture, drawing on the lessons learned across the national pilots to identify approaches that work for non-specialist employees in business environments where resources are often limited, increasing the exposure to threats.

4.2.1. INTEGRATE CYBERSECURITY AWARENESS INTO EXISTING SUPPORT AND ONBOARDING STRUCTURES

SMEs should be encouraged to embed basic cybersecurity awareness and hygiene practices into existing onboarding processes, training cycles, and continuous professional development frameworks for their employees. The modular, self-paced format of training programmes like CyberAgent makes this integration feasible even for microenterprises with limited training infrastructure and capacity. Business support intermediaries, including incubators and accelerators, can facilitate this by incorporating cybersecurity literacy into their standard SME development offer.

4.2.2. CYBERSECURITY TRAINING AS A BUSINESS IMPERATIVE

The CyberAgent pilot consistently showed that SME employees engage most effectively when training is built around concrete workplace relevance, answering the question of what cybersecurity means for their company, their role, and their daily work. The most effective SME delivery models were those that combined flexibility with practical, action-oriented content directly linked to everyday routines and tasks such as password practices, phishing awareness, safe data handling, and incident reporting. Future SME-facing cybersecurity upskilling should be designed around this concrete logic to increase the engagement of employees.

4.3. GENDER INCLUSION IN CYBERSECURITY

This section is directed at policymakers, training providers, funding bodies and industry organisations with a role in shaping who participates in cybersecurity education and workforce development. The recommendations build on the CyberAgent project's experience to propose concrete steps for closing the gender gap in cybersecurity training participation.

4.3.1. ADOPT GENDER-SENSITIVE RECRUITMENT AS A STANDARD PRACTICE

The Women4Cyber-led Belgian pilot demonstrated that deliberate, network-based, gender-sensitive recruitment can radically alter the participation profile of cybersecurity training. The result of the Belgian pilot should not be treated as an exceptional case but as evidence of what is achievable when gender inclusion is treated as a design requirement rather than a reporting metric or KPI. Cybersecurity training programmes seeking public funding should be required to demonstrate how their recruitment strategy actively reaches women, including women in non-technical roles.

4.3.2. FRAME CYBERSECURITY AS A GOVERNANCE AND AWARENESS CHALLENGE

The persistent underrepresentation of women in cybersecurity is reinforced, in part, by the field's dominant self-presentation as a highly technical, IT-specialist domain. Programmes and communications that put emphasis on cybersecurity governance, risk awareness and organisational culture, rather than only highlighting technical roles, are more effective at reaching women in managerial and administrative roles who have both the need and the capacity to engage with cybersecurity but do not see themselves reflected in conventional training offers. This framing shift costs nothing and has a measurable impact on participation.

CONCLUSION

The CyberAgent project demonstrated that the cybersecurity skills gap in European SMEs is not an unsolvable issue. By building a modular, workplace-relevant, and inclusive training offer, the project showed that non-specialist employees can develop meaningful cybersecurity competences, that women can be reached in significant numbers when inclusion is treated as a design requirement, and that the Cybersecurity Change Agent role can serve as a sustainable mechanism for embedding security culture within organisations that lack dedicated resources.

The EU policy landscape is moving in the same direction. The NIS2, the Cyber Resilience Act, the Digital Education Action Plan, and the Gender Equality Strategy collectively create both the obligation and the opportunity for exactly this kind of intervention. The consortium invites policymakers, training providers, and SMEs to engage with these findings, draw on the CyberAgent model, and contribute to shaping the next generation of inclusive, scalable cybersecurity training across Europe.

CyberAgent

Co-funded by the European Union

Get social with the project!

www.cyberagents.eu

contact@cyberagents.eu

@Cyber-Agent-EU

@CyberAgent.EU

@CyberAgentEU

@Cyber.Agent.EU

@CyberAgentEU

Project Partners

Vilniaus Universitetas 1579 Universitas Vilnensis

Kaunas Faculty

Prios

EVM Grupo

Teknopark İstanbul Mesleki ve Teknik Anadolu Lisesi

IT Akademija

ProxyLab

Women4Cyber European Cyber Security Organisation

Liceul Tehnologic Grigore C. Moisil Buzau