Co-funded by the European Union

GOOD PRACTICE GUIDE FOR SMES

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 6.4: Good Practice Guide for SMEs

Leader of WP6 – Women4Cyber Foundation

CONTENT

LIST OF TABLES

INTRODUCTION

The CyberAgent project was developed over three years across eight European countries: Romania, Belgium, Norway, Spain, Türkiye, Poland, Lithuania and Finland. CyberAgent was created to build and test a modular, accessible cybersecurity training programme for SME employees, VET learners, and HEI students. The central outcome of this work is the Cybersecurity Change Agent: a trained, non-specialist employee who acts as an internal point of reference for cybersecurity awareness within their organisation.

This Guide translates the project's implementation experience into practical guidance for SMEs. It explains what the Change Agent role is, how to identify and appoint the right person, how to support their training, and how to ensure that gender inclusion is embedded in the process from the very beginning. A checklist at the end helps SMEs verify that the right conditions are in place at each stage.

1. WHY CYBERSECURITY MATTERS FOR EVERY SME

According to the ENISA Threat Landscape 2025 report, cybercriminals are industrialising their attacks, making SMEs high-value targets regardless of their size and sector. The most common threats that organisations face today are ransomware, phishing, and data breaches. Ransomware and data breaches only account for the majority of cybercrime incidents targeting EU organisations, with ransomware accounting for more than 80% of crimes. The industrialisation of these attacks, notably the "Ransomware-as-a-Service" model, lowered the barriers for attackers, making even the smallest organisations viable targets.

For SMEs especially, the consequences of a cyberattack are not limited to temporary disruptions. According to ENISA, cybersecurity attacks have serious negative impacts on the businesses of 90% of the SMEs after one week of occurring. Yet, despite this exposure, SMEs rarely have dedicated IT or security staff, and their employees rarely receive structured cybersecurity training. SMEs in Europe employ around 100 million people and account for more than half of Europe's GDP. Therefore, the cybersecurity gap in the SME sector is an economic and societal risk.

Most cyberattacks succeed because of human factors such as a click on a phishing link, weak passwords, or unverified emails. This means that the first line of defence is not a technical tool, but an informed, aware employee who knows what to look out for and what to do when something goes wrong. This role is precisely the one covered by the Cybersecurity Change Agent.

2. THE CYBERSECURITY CHANGE AGENT

The concept of the Cybersecurity Change Agent sits at the heart of the CyberAgent project. This section explains what the role is, why it was developed, and what it looks like in practice within Small and Medium Enterprises (SMEs).

2.1. WHAT IS IT AND WHY IS IT NEEDED

SMEs are the backbone of the European economy, yet they remain among the most exposed organisation to cybersecurity threats. Unlike large companies, most SMEs do not have dedicated IT or security departments, and their employees rarely receive structured cybersecurity training. This results in a persistent gap between the cyber risks SMEs face and the capacity they have to tackle them.

The CyberAgent project and the Cybersecurity Change Agent figure were designed to address this gap by building a different kind of capability within existing teams. The Cybersecurity Change Agent is a trained, non-technical employee who acts as an internal reference for cybersecurity awareness, encouraging safer behaviour, recognising common risks, and implementing better cybersecurity practices within the organisation. This figure will also act as a guide for colleagues towards appropriate support in case of incidents.

The need for this role is confirmed by the evidence gathered throughout the CyberAgent pilot. Across eight partner countries, the training reached 594 registered participants spanning SME employees, HEI and VET learners. SME employees are commonly identified as the most difficult target group to reach and retain in educational settings, mainly due to time constraints and work responsibilities. Nevertheless, the high completion rate among SME employees reflects the genuine relevance of cybersecurity awareness in their day-to-day work.

2.2. CORE RESPONSIBILITIES

The Cybersecurity Change Agent is not responsible for solving cybersecurity problems alone. The role is built around awareness, communication, and coordination, being the person in the organisation who keeps cybersecurity on the agenda and helps colleagues navigate it in their daily work. None of this requires technical expertise. What it requires is someone trusted, well-connected within the organisation, and motivated to make cybersecurity a normal part of how the team works.

Concretely, the role translates into a set of recurring, lightweight activities that do not demand significant time but have a meaningful impact on the organisation's security culture:

- **Raising awareness on a regular basis**. The Change Agent shares regular awareness messages with colleagues on the most common threats such as phishing emails, weak passwords, unsafe data handling, suspicious links, keeping cybersecurity visible without turning it into a burden. This can be as simple as a monthly message shared on the team chat, a short reminder before a busy period, or a note about a new type of scam circulating in the sector. The format matters less than the consistency.

- **Keeping cybersecurity on the meeting agenda**. The Change Agent raises cybersecurity topics during team meetings through short, practical discussions. This does not mean lengthy presentations or formal training sessions. A five-minute conversation about a recent phishing attempt or a reminder about updating passwords is enough to keep awareness alive and signal that cybersecurity is a shared organisational responsibility, not something delegated to technical staff.

- **Encouraging incident reporting**. One of the most important contributions of the Cybersecurity Change Agent is creating a culture where employees feel comfortable reporting suspicious situations such as an unusual email, a system behaving unexpectedly, a colleague clicking on something they should not have. Many cybersecurity incidents escalate because employees do not report early warning signs out of fear of embarrassment or blame. The Change Agent helps normalise reporting by being approachable and clear about the process.

- **Supporting onboarding**. New employees are among the most vulnerable members of any organisation from a cybersecurity perspective because they are unfamiliar with internal procedures, more likely to trust unexpected requests, and often not yet trained on basic security practices. The Change Agent plays an important role in introducing cybersecurity basics during onboarding, ensuring that good habits are established from day one rather than retrofitted later.

- **Acting as an internal point of contact**. The Cybersecurity Change Agent is the person colleagues turn to when they have a cybersecurity question or are unsure what to do in a situation. This means they know where to find them, who to escalate to, and how to guide a colleague toward the right support. In SMEs without dedicated IT staff, this role fills a gap that would otherwise leave employees with no clear point of reference.

- **Promoting training and continuous learning**. The Change Agent encourages colleagues to engage with available training resources, including the CyberAgent modules, and stays informed about developments in the cybersecurity landscape relevant to the organisation's sector and activities.
- **Collecting and escalating feedback**. The Change Agent gathers feedback on cybersecurity concerns within the organisation about what employees find confusing, what practices are not being followed, what risks feel most pressing and brings these insights to management. This feedback loop is what allows the organisation to improve its security culture over time.

Table 1. Distinction between technical employees' tasks and Change Agent's tasks

IT SPECIALIST (Technical Role)	CYBERSECURITY CHANGE AGENT (Managerial & Cultural Role)
Configures firewalls and security systems	Shares tailored awareness messages and security alerts with colleagues
Manages software updates, patches, and technical configurations	Keeps cybersecurity consistently on the internal team meeting agendas
Responds to active cyber incidents and technical breaches	Encourages colleagues to actively and transparently report suspicious activities
Monitors network traffic, security logs, and technical compliance parameters	Supports new employees during the organizational onboarding process regarding baseline cyber hygiene
Implements technical security controls and manages infrastructure access	Collects ongoing feedback from staff and escalates systemic concerns to management or IT

3. SELECTING AND APPOINTING A CYBERSECURITY CHANGE AGENT

Identifying the right person for the Cybersecurity Change Agent role and giving them the conditions to succeed are crucial decisions to make when implementing the role within an organisation. The CyberAgent pilot showed that the role works best when it is filled by a person who is perceived as trusted, knowledgeable about the company's procedures, and supported by management. This section provides practical guidance on how to define the role clearly for long-term success and how to find the right candidate.

3.1. HOW TO IDENTIFY THE RIGHT CANDIDATE

Following the results of the CyberAgent pilot, the most effective Cybersecurity Change Agents are not necessarily those with a previous technical background. Across the eight pilot countries, SME participants who engaged most actively with the training and showed the greatest potential were those who combined organisational awareness with communication skills and genuine motivation to make the difference in their workplace. Based on the pilot experience, the following characteristics tend to support success in the role:

- Familiarity with the organisation's internal processes and data handling practices.
- Good communication and interpersonal skills.
- Support from management

Importantly, the role does not require a technical or IT background. Therefore, employees in administrative roles, HR, operations, and management can perform the Change Agent function effectively, provided they receive adequate training and support. Removing the technical prerequisite is a deliberate design choice that significantly widens the pool of eligible candidates and opens the door to gender diversity, as the pilot showed.

Once a candidate has been identified, the role needs to be made visible and legitimate within the organisation. The scope of the role should be announced across the organisation and should be clearly defined: what the Cybersecurity Change Agent is responsible for, who they report to, and what they are not expected to do.

3.2. IMPLEMENTING THE ROLE

The next step is implementing the role within an organisation. The following steps draw directly on the lessons learned from the CyberAgent pilot across partner countries and are designed to be proportionate for SMEs of any size.

3.2.1. SELECT AND TRAIN THE CYBERSECURITY CHANGE AGENT

Identify the most suitable person in your organisation and give them access to the CyberAgent training programme. The programme comprises nine modules covering Security Programme Management (M1), System Administration (M2), Analytical Tools (M3), Security Operations (M4), Security Governance and Policy (M5), Cybersecurity Planning (M6), Risk Management (M7), Business Continuity (M8) and Empowering Careers in Cybersecurity (M9). These nine modules are formally captured in two official project deliverables: D3.1, which covers the HEI curriculum, and D3.2, which covers the VET curriculum. The modules referenced throughout this Guide therefore correspond directly to the content described in D3.1 and D3.2 and can be accessed through the CyberAgent platform regardless of the learner's institutional affiliation. Moreover, the curriculum is aligned to EQF levels 4-6 for SME employees, providing foundational cybersecurity skills and knowledge with practical application across technical, analytical, risk management, and organisational competence areas.

The training is self-paced and available online, meaning the selected employee can complete it flexibly around their existing work responsibilities. Upon completing a module and passing the knowledge assessment test with a score of at least 75%, the Change Agent receives a Course Completion Certificate for that module, which provides a formal record of the competences acquired and can be used to document the Change Agent's training within the organisation.

3.2.2. DEFINE RESPONSIBILITIES AND INTEGRATE INTO EXISTING STRUCTURES

Once training is underway or complete, the organisation should formally define the Cybersecurity Change Agent's responsibilities and integrate the role into existing structures. This means agreeing on what the Change Agent will do, how much time they will dedicate to the role, and who they will coordinate with, and communicating this to the whole team.

The pilot showed that the Cybersecurity Change Agent role is most sustainable when it is connected to something that already exists in the organisation, rather than sitting in isolation. This could mean linking it to a regular team meeting agenda item or connecting it to an existing health and safety or compliance structure. The goal is to make cybersecurity awareness a normal part of how the day-to-day work and a shared organisational responsibility, not a separate activity.

3.2.3. BUILD INTERNAL AWARENESS AROUND THE ROLE

The Change Agent cannot operate effectively if colleagues do not know who they are or what they do. To give the selected employee the organisational legitimacy they need to function, it is necessary to send a clear internal communication outlining its role and responsibilities and organise regular meetings to allow employees to ask questions.

Beyond the initial announcement, the Change Agent should be encouraged to keep cybersecurity visible within the organisation through regular meetings. This does not mean lengthy training sessions or formal presentations. In the SME context, this could be done in the form of brief activities directly connected to situations employes recognise from their daily work.

3.2.4. REGULARLY REVIEW AND SUSTAIN OVER TIME

To allow the Cybersecurity Change Agent role to generate lasting impact, the organisation needs to create the conditions for it to continue and evolve. This means building in a review process at least once a year, to assess what is working, what gaps remain, and whether the Change Agent needs additional training or support.

The pilot evidence shows that sustained engagement requires more than initial training. SME participants consistently need flexible deadlines, reminders, and occasional support to maintain momentum. Building in a simple annual review and ensuring the Change Agent has ongoing access to resources are the minimum conditions for keeping the role effective over time.

4. GENDER BALANCE AND INCLUSIVITY

Cybersecurity remains one of the most male-dominated fields in the European economy. Women represent approximately 20% of the cybersecurity workforce across the EU, and participation in cybersecurity training reflects the same imbalance. Due to the existing skills and talent gap, a field that draws from only a fraction of the available pool will struggle to meet the scale of demand that the current threat landscape requires.

The CyberAgent project was designed with gender inclusion as an explicit objective, not an afterthought. In a field where women typically account for a small minority of training participants, the high number of women participants to the pilot is a meaningful result and it was the product of targeted outreach strategies and inclusive framing.

4.1. WHY IT MATTERS FOR SMES

For SMEs specifically, the gender dimension of cybersecurity is both a workforce issue and an organisational culture issue. Most SMEs do not have dedicated cybersecurity staff. Their cyber resilience depends on the awareness and behaviour of all employees, especially those in administrative, HR, finance, and operations roles. Therefore, excluding women from cybersecurity awareness training is a security gap.

At the same time, the Cybersecurity Change Agent role offers a concrete opportunity to address the gender imbalance in cybersecurity from within SMEs. Because the role is defined by communication skills, organisational awareness, and governance thinking rather than technical expertise, it is well suite to a broad range of professional profiles and it offers women in non-technical roles a recognised pathway into cybersecurity responsibility that does not require a career change or a technical qualification.

4.2. PRACTICAL STEPS TO REACH WOMEN AND UNDERREPRESENTED GROUPS

The following practical steps are drawn from the CyberAgent pilot experience and are designed to be implementable by SMEs of any size.

The Belgian pilot demonstrated that channelling outreach through networks that women already trust, such as professional associations and business women's networks, increases female participation. In practice, this means that when an SME is identifying candidates for the Cybersecurity Change Agent role, it should actively engage any women's professional networks relevant to its sector or region, rather than relying solely on public announcements.

Frame the role in terms of organisational impact, not technical expertise. Women in non-technical roles are more likely to engage with cybersecurity training and take on the Change Agent function when the role is presented in terms of the organisational value it brings rather than in terms of technical skills. The role can be framed as one that protects the business, supports colleagues, and contributes to governance. The language used in internal communications, job descriptions, and recruitment materials matters.

5. BEST PRACTICES

Appointing a Cybersecurity Change Agent is an important first step, but the role can only generate lasting impact if it operates within an organisational culture that actively supports it. The following best practices are designed to help SMEs create the right conditions for the Change Agent to succeed and for cybersecurity awareness to become a normal part of how the organisation works.

- **Encourage open communication**. Employees should feel comfortable reporting mistakes, suspicious situations, or security concerns without fear of blame or embarrassment. In many organisations, cybersecurity incidents escalate precisely because employees hesitate to report something they are unsure about or feel responsible for.

- **Keep it simple and embedded in daily routines**. Cybersecurity awareness does not need to take the form of formal training sessions or lengthy workshops. Brief, practical reminders embedded in existing routines are often more effective than occasional intensive training. The goal is to make cybersecurity a background habit rather than a periodic event.

- **Document every step of the way**. One of the most practical steps an SME can take is to write down its basic cybersecurity practices: how passwords are managed, how sensitive data is stored and shared, what to do when a suspicious email arrives, who to contact in case of an incident. These do not need to be formal policy documents. A one-page reference accessible to all employees is enough.

- **Start at the top**. The behaviours expected of employees need to be visibly modelled by managers and leadership. If management does not follow basic security practices, it sends a signal that these practices are optional. The Change Agent's credibility within the organisation depends in part on whether the culture around them supports what they are trying to promote.

- **Make awareness continuous**. Cybersecurity threats evolve constantly, and a single training session becomes outdated quickly. Awareness needs to be treated as an ongoing process rather than a one-time activity. This means regular touchpoints, periodic refreshers, and a Cybersecurity Change Agent who stays informed and keeps bringing relevant information back into the organisation.

5.1. QUALITATIVE INPUT FROM THE NATIONAL PILOTS

The qualitative feedback shows that participants were generally positive about the training, with many stating that no major improvements were needed. The most repeated themes in open text responses (D5.3 - CyberAgent upskilling Training Program Evaluation) were: platform usability, navigation or assessment flow; technical access or reliability issues; positive value around accessibility, flexibility and broad knowledge; requests for more practical cases, hands-on labs or real SME examples; content density, structure or learning-path differentiation. Notably, the third most mentioned theme (positive value around accessibility, flexibility and broad knowledge) reflects appreciation from participants who stated that no improvements were needed and highlighted the programme's strengths unprompted. This is a meaningful signal: in an open text field designed to capture criticism, nearly a quarter of qualitative responses expressed satisfaction with the training's accessibility and breadth.

5.2. ACTION POINTS FOR IMPLEMENTING AND MANAGING THE TRAINING WITHIN SMES

The large-scale piloting of the CyberAgent platform across eight European countries provided key insights into how small and medium-sized enterprises absorb and maintain cybersecurity upskilling. Based on the mixed-method evidence and learner barriers documented in the final training evaluation report (D5.3), enterprise managers are recommended to adopt the following internal management, technical, and strategic action points to optimize the training's organizational impact.

Quality Management Advice

The CyberAgent learning materials present a substantial volume of operational and strategic knowledge. Managers should avoid assigning the entire curriculum at once; instead, establishing a modular schedule prevents cognitive fatigue and ensures a smoother capability transition into the company's daily routines.

Technical Integration Advice

Initial pilot data logged that technical onboarding friction, such as delayed or filtered platform registration confirmation emails, can hinder early adoption. Before rolling out user enrolment, management should coordinate with their network filters to ensure external e-learning domain paths are fully permitted and advise staff to monitor baseline spam folders.

Strategic Deployment Advice

The national piloting data revealed that higher-level strategic modules – specifically M6 (Cybersecurity Planning) and M8 (Business Continuity) – require solid background experience to be fully leveraged. To maximize immediate business value, these modules should be targeted specifically at personnel with managerial, operational, or business governance responsibilities.

5.2.1. VOICE OF THE CHANGE AGENT

The piloting phase, which aggregated 272 comprehensive survey responses across eight European countries, revealed three cross-cutting impacts on the target groups.

High Delivery Flexibility and Work-Study Balance

A significant 86.0% of respondents agreed or strongly agreed that the asynchronous, self-paced format was sufficiently flexible to be seamlessly integrated into their professional and academic schedules, allowing SME employees to balance competence building with daily operational duties.

Methodological Relevance for Non-Technical Personnel

The pilot outcomes validate the core educational design of the CyberAgent curriculum, proving that effective organizational cyber resilience does not require advanced technical or IT programming skills. According to the impact evaluation data in D5.3, 77.2% of participants reported that the training enabled them to clearly understand how their specific professional roles influence and protect daily security practices within an enterprise.

Measurable Knowledge Progression from Non-Expert Baselines

Platform analytics show that 89.3% of all participants achieved a verified increase in their cybersecurity knowledge. Crucially, this progression was most visible among absolute beginners: 90.9% of learners who evaluated their initial understanding as “Very Low” before the programme reported a decisive upgrade in their knowledge and confidence to recognize corporate cyber risks.

5.2.2. "DOS AND DON'TS"

Based on the feedback from the pilot countries regarding "learning-path differentiation", we present recommendations for companies:

Table 2 "Dos and Don'ts"

DO NOT (SME Pitfalls)	RECOMMENDED (Best Practice)
Expecting that an employee will listen to all 8 modules within an unrealistic, compressed timeframe (e.g., one week or month). Pilot studies (D5.3) revealed that a lack of time due to daily work responsibilities was the main barrier for SME employees, leading to a lower test pass rate.	Creating a flexible, individual learning schedule based on the employee's needs and availability, applying micro-learning principles. Allow learners to focus on modules that directly enhance their specific area of workplace impact.
Expecting that the trained Cybersecurity Change Agent will replace specialized IT engineering or independently resolve complex cyber incidents. Shifting core technical infrastructure expectations onto non-technical staff creates heavy role ambiguity.	Encouraging the Change Agent to act as an internal security coordinator and awareness catalyst. They are most effective when driving safety culture, internal training reminders, and running brief updates during team meetings.
Leaving the e-learning process completely unmonitored to run on autopilot without corporate visibility. A single registration link does not guarantee long-term organizational value.	Utilizing the structured monitoring framework (such as Table 3) to track milestones and assigning internal mentoring. Pointers from the pilot evaluation (D5.3) confirm that having a designated manager or mentor explicitly correlates with verified test finalization.
Allowing independent study to run in total isolation, risking that individual learning blocks or hidden tech difficulties remain unnoticed. Without interaction, absolute beginners often stall and silently abandon the program when stuck.	Integrating self-paced study with proactive operational touchpoints, such as short pulse checks or digital reminders. Active management alignment directly dismantles learning barriers, lifting employee motivation and course completion rates.

6. ROADMAP TO IMPLEMENT THE CYBERSECURITY CHANGE AGENT

Implementing the Cybersecurity Change Agent role successfully starts well before the appointment itself. Taking the time to assess the organisation's current situation, build internal support, and define the role clearly from the outset significantly increases the chances of long-term success. The following steps are designed to practically guide SMEs through this preparation phase.

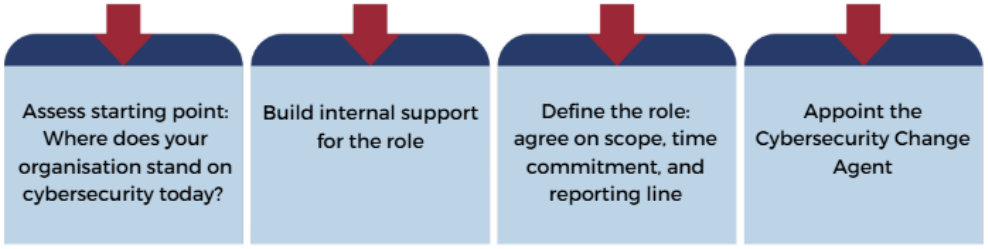
1. The first step is to assess where the organisation currently stands. This means taking an honest look at the cybersecurity practices already in place, or absent. Are employees aware of basic threats such as phishing? Is there a procedure for reporting suspicious incidents? Is sensitive data handled consistently across the team?

2. The second step is to build internal support for the role. The Change Agent cannot operate effectively without management backing. Before selecting a candidate, the decision to introduce the role should be discussed and agreed at management level, with a clear commitment to allocating time, recognising the role formally, and actively supporting the person who takes it on.

3. The third step is to define the role before filling it. This means agreeing on the scope of responsibilities, the time commitment expected, and how the role will sit within the existing organisational structure. A clear mandate, even a simple one-paragraph description, avoids ambiguity and gives the future Cybersecurity Change Agent the legitimacy they need to act.

Only once these three steps are in place is the organisation ready to identify and appoint the right candidate. The following section outlines the checklist that will guide the successful implementation of the role.

Figure 1 - Visual Roadmap to implement the cybersecurity change agent



7. CHECKLIST

The following checklist is meant to be used to verify whether the key conditions for a successful Cybersecurity Change Agent implementation are in place. It is based on the lessons learned from the CyberAgent pilot.

7.1. MANAGEMENT

[ ] The Change Agent role has been formally agreed and budgeted for

[ ] A clear mandate has been defined: scope, time commitment, and reporting line

[ ] The appointment has been communicated to the whole organisation

[ ] A review of the role has been scheduled within the next 12 months

[ ] The Change Agent has protected time in their schedule to carry out the role

7.2. HUMAN RESOURCES

[ ] The selection process was open to all people, regardless of gender or background

[ ] The role was communicated in terms of organisational impact, not technical expertise

[ ] The Change Agent's responsibilities have been reflected in their job description or objectives

[ ] New employees are introduced to the Cybersecurity Change Agent during onboarding

[ ] A record of the Change Agent's training and certifications is kept

7.3. CYBERSECURITY CHANGE AGENT

[ ] Registered on the CyberAgent platform and agreed on a learning pathway

[ ] Completed at least one module and obtained a certificate

[ ] Colleagues know how to get in touch with the Change Agent

[ ] Basic cybersecurity practices are documented and accessible to all staff

[ ] Regular awareness touchpoints are in place (meetings, messages, or reminders)

[ ] A clear process exists for colleagues to report suspicious situations

[ ] Feedback on cybersecurity concerns is collected and escalated to management regularly

8. HOW TO MEASURE A SUCCESSFUL IMPLEMENTATION

Implementing the role of the Cybersecurity Change Agent is an ongoing commitment. The following indicators can help SMEs assess whether the role is having a real impact over time.

[ ] The number of employees participating in cybersecurity awareness activities has increased since the Change Agent was appointed

[ ] Cybersecurity is raised regularly in team meetings and is no longer treated as an exceptional topic

[ ] Employees know who the Change Agent is and feel comfortable approaching them with questions or concerns

[ ] The number of reported suspicious emails, incidents or concerns has increased

[ ] The Change Agent has completed additional training modules since their initial appointment

[ ] Staff feedback on cybersecurity within the organisation is collected periodically and acted upon

8.1. MANAGERIAL GUIDANCE FOR TEMPLATE ADAPTATION AND CUSTOMIZATION

To ensure that the upskilling of your Cybersecurity Change Agent transfers into long-term corporate resilience, continuous structural monitoring is essential. Table 3 provides a practical tracking template designed for SME managers to evaluate organizational baseline levels before training and measure concrete safety culture progression at 6 and 12 months post-appointment.

Managers should treat this template as a dynamic framework. Depending on your enterprise's size, operational sector, and existing infrastructure, you are encouraged to adapt and expand this matrix:

- **Customizing Scales**
  Micro-SMEs (under 10 employees) may simplify percentage-based metrics into direct employee counts to maintain ease of tracking.
- **Expanding Indicators**
  Enterprises operating in highly digitized or high-risk environments are recommended to add target-specific rows, such as “% of staff utilizing multi-factor authentication (MFA)” or “Average response time to a simulated threat.”
- **Localization**
  Align the “Recommended Data Source” column with your specific internal communication channels (e.g., tracking via Slack, MS Teams polls, or physical logs during team briefings).

Table 3. Post-Appointment Tracking Template for SME Managers

Success Indicator	Unit / Measurement Scale	Baseline (Before)	Progress (6 Months)	Target (12 Months)	Recommended Data Source
Employee Phishing Readiness	% of staff confident in handling suspicious emails	%	%	%	Internal pulse survey or CyberAgent platform data
Meeting Integration Frequency	Number of team meetings where cybersecurity was raised	Count	Count	Count	Team meeting minutes/agendas
Incident Reporting Active Rate	Number of documented suspicious incidents reported	Count / month	Count / month	Count / month	Internal security incident log or IT feedback loop
Change Agent Visibility	% of staff who accurately know who the Change Agent is	%	%	%	Short internal questionnaire
Platform Progress Commitment	Number of employees actively engaged in micro-learning	Count	Count	Count	CyberAgent platform manager analytics dashboard

CONCLUSION

Cybersecurity is no longer a concern reserved for large organisations with dedicated IT departments. As the threat landscape continues to evolve and regulatory expectations on SMEs increase, the question is how they can defend themselves with the resources they actually have.

The Cybersecurity Change Agent role offers a practical and proportionate answer to that question. It does not require hiring a specialist, investing in expensive tools, or overhauling existing processes. It requires identifying the right person within the organisation, giving them the training and the mandate to act, and creating the conditions for cybersecurity awareness to become part of everyday working life.

The CyberAgent project has shown that this is achievable. Across eight European countries, SME employees with no technical background completed the training, took on the role, and began making a difference in how their organisations approached cybersecurity. The evidence is clear: when the barrier to entry is lowered, when the role is framed around organisational culture rather than technical expertise, and when inclusion is treated as a design principle rather than an afterthought, the results follow.

This Guide is an invitation to take that first step. The roadmap is there. The tools are available. The role is within reach for any SME willing to invest in its people.

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