Digital Skills & Jobs Platform

Towards organisational cyber resilience: strategies for cybersecurity skills training and enhancing awareness of cyber threats

The Digital Brief series dive deep into the latest trends and topics in the area of digital skills and jobs and are produced in collaboration with proven experts in the field.

The Digital Skills and Jobs Platform is funded by the Digital Europe Programme of the European Union. Opinions expressed do not necessarily reflect the contracting authority’s official position.

Table of Contents

Subtitle

This paper presents strategies for building cybersecurity skills and awareness aligned with business goals. It stresses the need to protect critical assets through tailored training based on risk assessments where training are a critical security component of the overall security architecture.

Key elements include understanding threats, attack vectors, and the organisation's attack surface. Establishing a cybersecurity baseline and fostering the security culture are essential for organisational resilience across its operational activities.

Summary

This brief outlines strategies for developing cybersecurity skills and raising awareness of cyber threats in a way that corresponds to organisational business objectives and operational context. It first dives into the role of digital competencies as the necessary foundation to enhance core capabilities in the field of cybersecurity and moves on to explore why we need to understand what we need to protect to ensure effective training.

Cybersecurity efforts should be guided by a risk analysis, an understanding of the threat landscape, and a clear assessment of the organisation's attack surface (i.e. the area that the Organisation can be attacked on. Developing advance cybersecurity skills to minimise this attack surface translates into safety on an organisational level). What is more, tailored protection measures must be applied to each asset (i.e. the thing we have to protect), reflecting its unique value and vulnerability.

Cybersecurity training is not merely procedural but rather forms a strategic framework within information security governance that increases security readiness. Establishing a baseline level of cybersecurity through awareness programs is a foundational step. These programs foster a culture of vigilance, enabling employees to identify and respond to threats effectively. A number of EU and national-level initiatives aim to foster the development of cybersecurity skills for European workforce and citizens, and this brief lists some of the most impactful ones in one of its chapters.

Finally, this article sets the stage for further discussion on targeted strategies to build organisational resilience against cyberthreats in a consistent, time-effective manner as part of the overall security governance and the relevant security architecture, concatenating across the different domains of interest of the organisation.

Keywords

Cyber skills, threat awareness, digital competence, business objectives, critical assets, time value, risk analysis, attack vectors, mitigation, awareness.

Author's biography

Dr. Marios Thoma is a retired military officer, having achieved the rank of Colonel in signals. He commenced his military career after graduating from the Hellenic Military Academy and joining the National Guard of Cyprus in 1997. He holds a Master of Science degree in communications and computer science from the University of Athens, Greece, and is a graduate of the Hellenic Military School of Signals Officers, specializing in Telecommunications and Electronics.

In 2018, he obtained his PhD degree from the Department of Electrical and Computer Engineering at the University of Cyprus. His doctoral research focuses on cyberspace defence, particularly on modelling and early detection techniques for cyber attacks, with a specific emphasis on Advanced Persistent Threats (APTs).

Throughout his career, Dr. Thoma has amassed significant expertise across various domains such as Information Assurance, Development Security Operations, Cyber Security Engineering, Data Governance, and Information Security Management. He has been involved in a multitude of projects, ranging from accrediting Communication Information Systems to crafting Business Continuity and Recovery Plans. Furthermore, his knowledge extends to Hybrid Threats and Space, particularly in conjunction with Cybersecurity.

He is an IEEE Senior Member and serves as a national representative in specialized committees and organisations, including CEN/CLC/C47X, European Technical Standardisation Institute (ETSI) in the Technical Committees for (1) Securing Artificial Intelligence (SAI), (2) CYBER/PQC, and (3) QKD.

Moreover Dr. Thoma has actively participated in strategic, operational, and technical endeavours within both national and EU contexts.

He is currently the Director of Cyberecocul Global Services - a newly-founded startup dedicated to providing cybersecurity services across research, development, and innovation, with a strong focus on Space, AI, and Quantum.

Introduction

This paper offers a high-level overview of approaches for building cybersecurity skills and raising awareness of cyber threats. It presents examples that illustrate how digital competencies can enhance an organisation's core capabilities and support secure operations.

Although significant emphasis has been placed on Network and Information Security (see the NIS2 Directive) and cyber skills development within the EU (see the European Cybersecurity Skills Framework), a substantial amount of work remains to be done.

In terms of security, any organisation's day-to-day operations are guided by its business objectives, which define what matters most. It is the organisation's business objectives that 1) set the scope of the organisation's activities and 2) guide the level and direction of the expertise and talent required. Understanding these objectives is essential when developing cybersecurity skills tailored to the needs of companies, as they ultimately inform how to protect the organisation's critical assets—whether tangible or intangible. This overall architecture is an integral part of the information security governance of the organisation.

Amongst these critical assets, and as the organisation continues its activities, **time stands out as particularly valuable.** It is **non-renewable** and **non-recoverable**, making its management a high-priority concern. Activities that involve managing or optimising time are often complex and difficult to implement. Cybersecurity training is one such time-intensive activity: for it to be effective, it must be aligned with the organisation's specific goals and operational needs as part of the information security governance. Indeed, each and every asset within an organisation has unique characteristics and requires tailored protection measures to ensure its security. **Developing cybersecurity skills is not just a training exercise—it creates a strategic framework for protecting these critical assets in an intelligent and efficient manner via respective security measures.**

To design relevant training programs, it is essential to first understand what needs to be protected in the business. This clarity is crucial for identifying the type and scope of training required within an organisational context. **Moreover, cyber threats and the corresponding attack vectors—manifesting in various forms—must be identified and accurately assessed.** This enables the implementation of appropriate mitigation measures. A thorough risk analysis, along with an understanding of the organisation's threat landscape, is fundamental to this process. Equally important is identifying and addressing the organisation's attack surface, which represents potential entry points for cyberattacks.

Establishing a baseline level of cybersecurity is a critical first step in building a coherent skills development strategy. This is where cybersecurity awareness programs play a pivotal role. Their primary function is to instil a culture of awareness throughout the organisation, enabling employees not only to recognize potential threats but also to act responsibly and report incidents appropriately.

The following chapters will further examine the key terms introduced above and present strategies for cybersecurity skills training that are tailored to organisational needs, aimed at strengthening defences against cyberthreats always in line with the business objectives of the organisation.

The Idea - Scope & Objectives

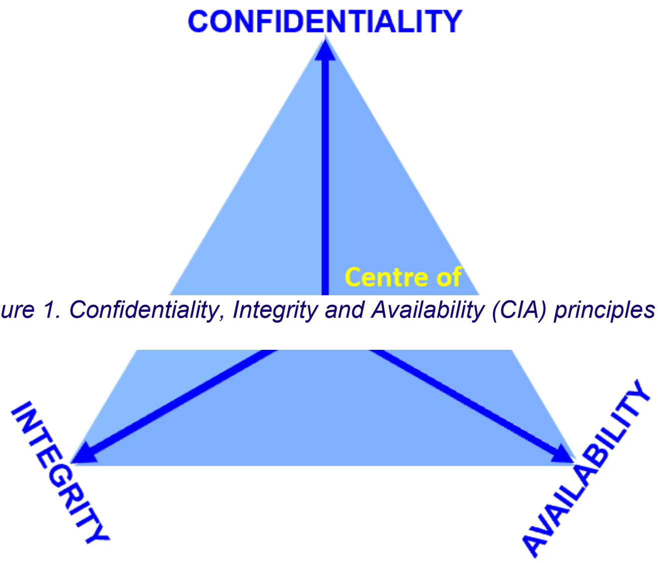


Figure 1. Confidentiality, Integrity and Availability (CIA) principles

The centre of gravity in security for an organisation defers based on the **Confidentiality, Integrity and Availability (CIA) principles** (see Figure 1. Confidentiality, Integrity and Availability (CIA) principles). This is vital for any further security analysis.

These concepts define the information security and the security governance of the organisation. The Business Objectives are interlinked with the security triad. Each organisation must clearly identify and define the interdependencies of the security triad with its core business accordingly. Moreover, an organisation's main activities in cybersecurity can be categorised across 4 primary levels: **strategic, tactical, operational,** and **technical.** Taken together, these levels form a comprehensive ecosystem of actions that support the organisation's overall cybersecurity posture across all of its activities. The security triad is a key part of this process.

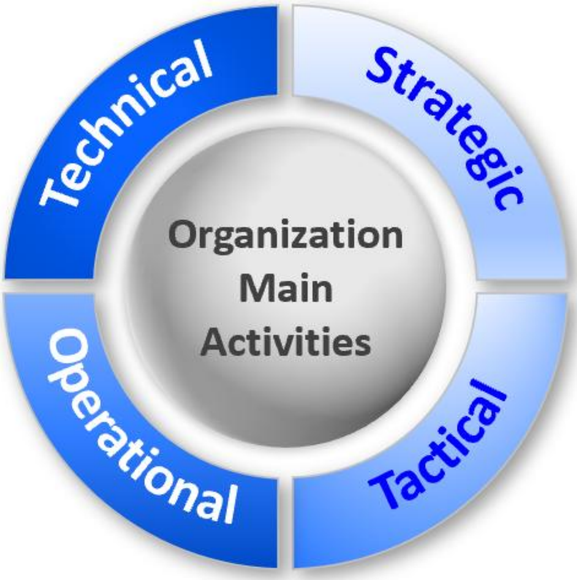
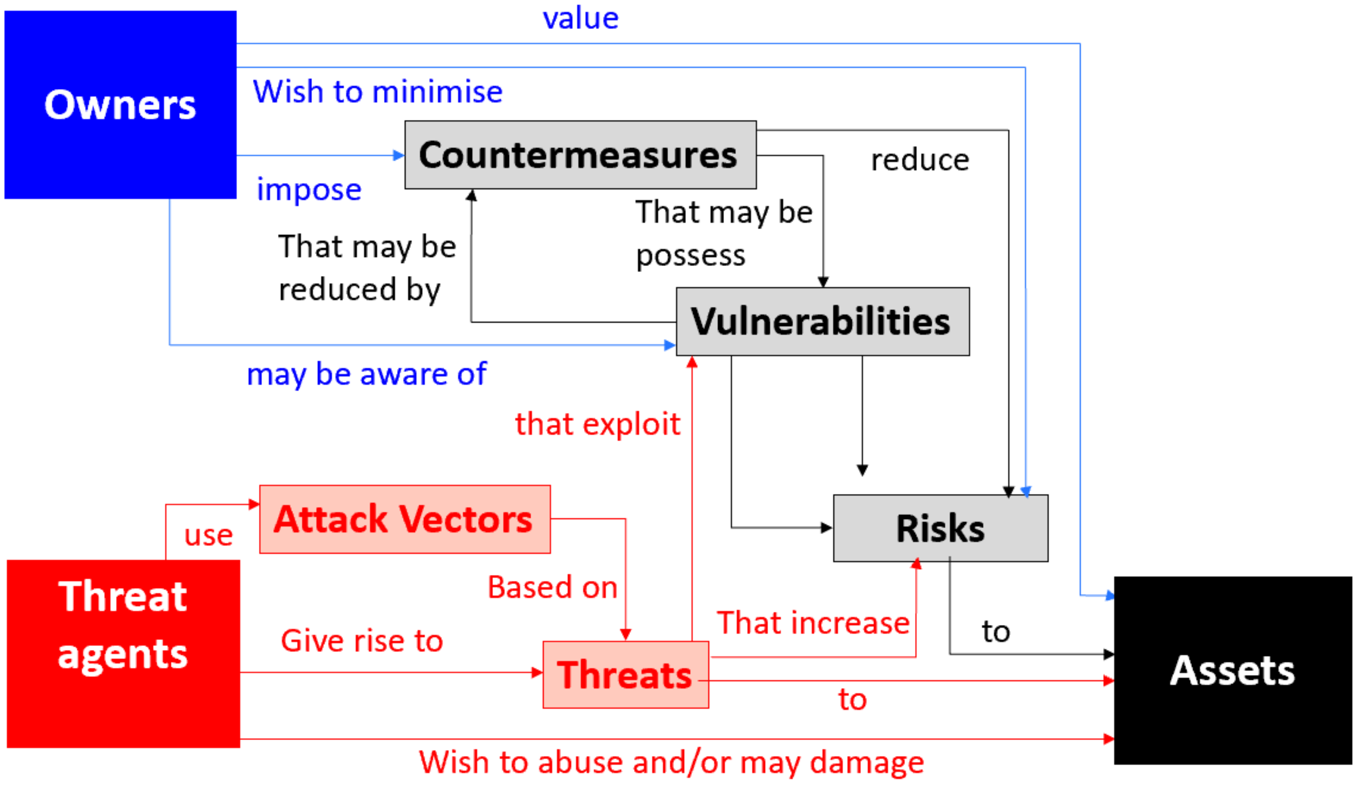


Figure 2. An axis of an organisation's main activities

Information security plays a vital role in minimising risks, ensuring business continuity, and enhancing both return on investment and opportunities for growth. Within this framework, the organisation must effectively direct and manage activities across the three key management levels: Strategic, Operational and Tactical (Solms and Solms, 2006).

The overarching goal is to align these management levels with core activities and the development of cybersecurity competencies. Developing cyber skills is a critical part of this process and should be embedded within the organisation's value chain. This ensures consistency with business objectives and enhances the organisation's cybersecurity resilience.

Asset (Vulnerabilities, Controls), Threat (Threat Agent Profile, Likelihood) and Impact.



Schema 1: ENISA report 2017 ,The elements of risk and their relationships according to ISO 15408:2005

All Organisations should implement cybersecurity initiatives across the strategic, operational, tactical and technical levels. Embedding cyber skills development within the value chain ensures alignment with business goals. Robust information security reduces risks, supports continuity, and drives growth. Effective coordination across all management levels is essential to build a resilient and security-conscious culture. Training and awareness efforts must be tailored to safeguard assets (what we have to protect) and address the organisation's unique threat environment. There are several activities we can undertake in this context, such as:

- Develop cybersecurity skills within the organisation to align with its business objectives and operational needs.
- Enhance awareness of cyber threats across all levels of the organisation to foster a proactive security culture.
- Establish a baseline level of cybersecurity as a foundational step toward building a resilient and informed workforce.
- Protect critical organisational assets—both tangible (e.g., IT systems, infrastructure) and intangible (e.g., time, knowledge, data)—through strategic training and awareness.
- Adapt cybersecurity strategies to reflect the specific risk landscape and threat vectors faced by the organisation.

The Current Threat Environment – State of Play

If we took a more in-depth look at the real threat environment (as we face it now), we would see it consists of a number of threats that permeate virtually all of the activities that take place in an organisational context (see ENISA 2017, ENISA 2024). These threats can materialise in various ways, but regardless, have an impact on the core business of each company and organisation. This adds an additional layer of responsibility for the organisation, as efforts should be concentrated in understanding what is needed for the organisation to protect itself in a coherent way, and also what threats to prioritise.

It is this prioritisation that is the key element for success. Not everything has the same impact - and not everything is urgent – rather, processes can be regarded as part of the whole value chain of an organisation. (i.e. those activities that can add real value to the organisation). In this regard, it is pivotal for the organisation to define the critical elements of its value chain – and accurately identify the threat vectors that interact with these critical elements in order for them to be addressed. Imagine a competent security analyst of a financial institution, who fails to perform regular monitoring to assess the level of security on a continuous approach for said financial institution. This is considered a major weakness since it can potentially affect the value chain of the financial services of the institution.

Amongst the most important threat vectors that are engaging with the overall activity of an organisation is 'human' interaction. In an organisational context, the personnel engages in operational activities across several aspects – at **Strategic, Operational, Tactical** and **Technical** levels through a number of actions. People are the driving force that can propel an organisation to succeed – or fail. Well-educated and properly trained staff can make all the difference. Therefore, depending on skills levels and awareness, personnel either can be seen as a lethal 'attack vector' or as a vital 'countermeasure'.

The AI Component – Risks and Opportunities

As cyber threats—particularly Advanced Persistent Threats (APTs) [1]- become more stealthy, adaptive, and resourceful, integrating Artificial Intelligence (AI) into cybersecurity operations offers a transformative opportunity. AI is not only capable of enhancing detection and response capabilities, but also shifts cybersecurity paradigms from reactive to proactive defence models. This concept can support and boost the design, development and implementation of target oriented training tailored to the business objectives.

AI offers powerful capabilities but also introduces certain security risks, as acknowledged by the European Commission in the AI Act. The integration of the Act into cybersecurity brings substantial challenges that require the development of a specialised cyber skill framework. Since AI systems are susceptible to threats like model poisoning and adversarial attacks and require expertise in secure model development, validation, and explainability, it is beneficial for the organisation to adopt a security-by-design mindset.

Retrofitting AI into legacy infrastructure without holistic planning and without the appropriate skill development can introduce great vulnerabilities. This brings the need for skills in system-level redesign and AI integration to the very forefront of all activities and efforts in this area. Furthermore, the slow and complex process of AI standardisation demands that cybersecurity Organisations' personnel stay adaptable and continue to engage with the evolving and fragmented compliance landscapes. Aligning AI-based cyber

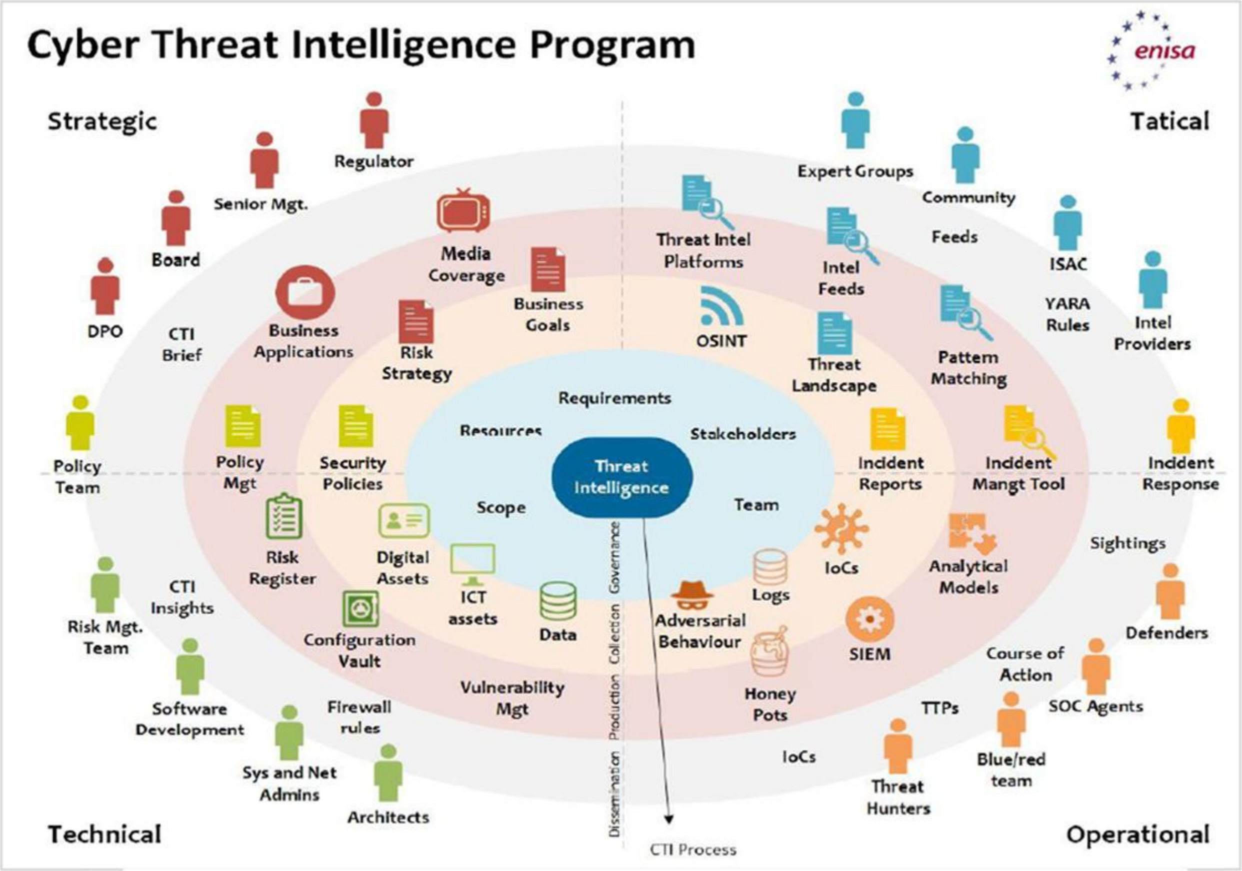
[1] *APTs are sophisticated, unknown threats that are considered amongst the most dangerous types of cyber threats. They are difficult to detect and, in most cases, remain unnoticed for long after breaching an organisation's systems. In most cases, APTs carry out highly damaging cyberattacks that result in the highest financial and operational costs for organisations.*

tools with legal and ethical frameworks—such as the EU AI Act – within an entity's operational activities requires knowledge of transparency requirements, risk classification, and human oversight, which in reality should involve all staff of an organisation, across their various levels.

As a result, cyber skills training must expand beyond traditional domains to include AI-specific security practices, legal literacy, and interdisciplinary coordination to ensure secure, ethical, and reliable deployment of AI in the security operations of the organisation.

The Methodology – what we have to do and how

The effectiveness of strategies for cybersecurity skills training and enhanced awareness of cyber threats should be based on the real threat environment and the type of threats that need to be addressed.



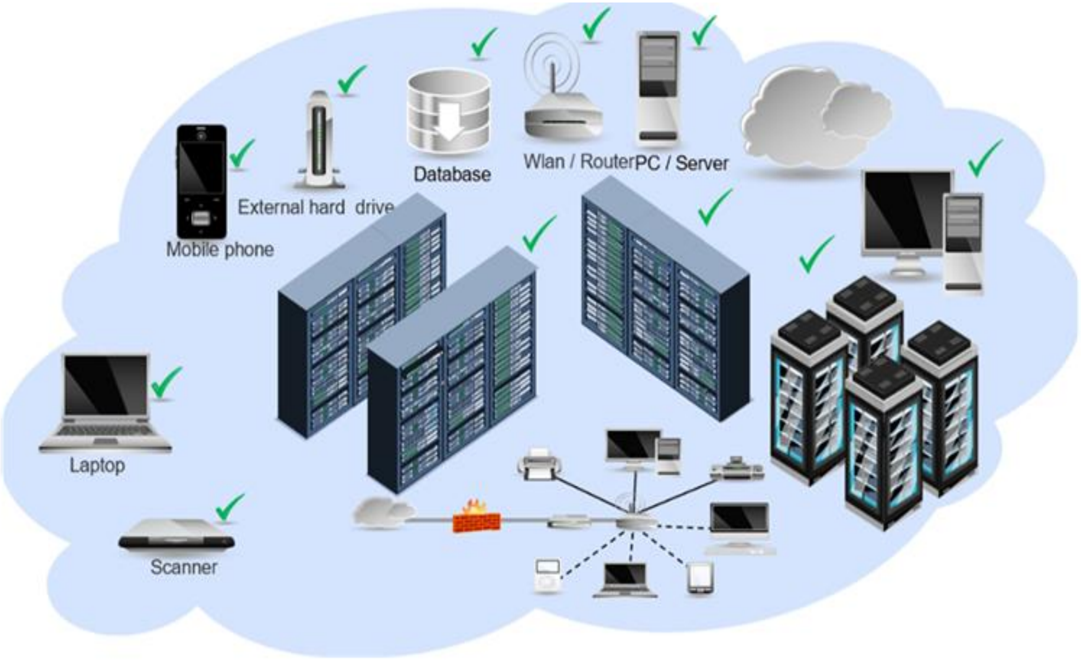
Schema 2 : Cyberthreat Intelligence Program representation [3]

In this regard the Cyber Threat Intelligence of ENISA (i.e. annual threat landscape reports) plays a crucial role. In reality, this sets the baseline of the defensive directions that need to be followed through the ecosystem of the organisation.

Without insight into the cyber threat landscape, defensive actions and countermeasures lack focus, specificity, and effectiveness —directly leading to significant weaknesses in the incident response process.

ENISA's Threat Landscape reports are also split across 4 main categories or levels - Strategic, Operational, Tactical and Technical. Each level plays a pivotal role in the information security governance and the overall security architecture of the organisation.

Moreover, the specific activities need to be tailored to specific challenges, across certain lines of developments and during the process need to be monitored via specific Key Performance Indicators (KPIs) based on the identified Key Goal Indicators (KGIs). Mitigation actions should also be foreseen based on Key Risk Indicators (KRIs). Key Risk Indicators heavily engage also with the infrastructure an organisation has at its disposal, and the related Communication Information Systems (CIS), including how these are operated and managed.



Schema 3 : Communication Information Systems of an Organization

In this regard, the problem of the development of cyber skills need to be seen as a framework of actions based on a risk priority approach in-line with the operational environment of the organisation taking into account the realistic threats, the related thread vectors and the identified attack subphase of the organisation .

The continuous engagement of the management in the whole process is vital.

- Potential challenges that may affect the implementation of cybersecurity training and awareness programs include, but are not limited to:
  - Support from management.
  - Time constraints – training competes with routine operational duties.
  - Alignment with business objectives – ensuring training reflects the organisation's goals and critical asset protection needs.
  - Diverse and evolving threat vectors – requiring constant content updates and vigilance.
  - Employee engagement – sustaining interest and participation over time.

  - Resource limitations –budget, staffing, and infrastructure constraints may hinder scope and frequency.
  - Key Lines of Development.
  - The absence of budget.
- To make cyber skills development both realistic and effective, organisations should follow several key development lines:
  - Strategic planning on the allocation of the recourses and on the budget planning.
  - Assessment of organisational assets to identify risk exposure and corresponding training needs.
  - Tailored training programs that address specific functions and departmental roles.
  - Integration of risk analysis and threat modelling into training content to promote proactive defence thinking.
  - Deployment of cyber awareness programs that foster a strong foundation in cyber hygiene and incident response.
  - Continuous improvement cycles using feedback and threat intelligence to refine training and awareness strategies.

- Monitoring and Metrics. Evaluating the impact and effectiveness of cybersecurity skills training is essential. This requires a set of actionable and regularly updated KPIs that reflect the actual operational environment. These may include, but are not limited to:
  - Training completion rates across departments and roles.
  - Performance in phishing simulations, such as reduced click-through rates on test emails.
  - Employee reporting rates, such as an increase in early identification and flagging of suspicious activity.
  - Time-to-respond and recovery following cybersecurity incidents.
  - Percentage of staff with role-specific cybersecurity competencies, distinguishing between technical personnel and general staff.

EU and national efforts in the realm of cyber

Building resilience and capacity in the field of cybersecurity has long been a priority of the European Union, yet efforts on both EU and national level have been boosted in recent years. The Digital Europe Programme of the European Union dedicates a substantial amount of funding for the development of advanced cybersecurity skills. Just for the period from 2023 to 2024, €375 million via the Digital Europe Programme were directed towards enhancing the EU's collective resilience against cyber threats. In 2024, the European Commission announced that €145.5 million would be made available to European SMEs and public administrations to support them in developing advanced cybersecurity solutions to optimise work processes and integrate best practices from the latest cutting-edge studies and research.

Several projects financed by the Digital Europe Programme are equally placing a strong emphasis on the area of cyber skills development. The CYRUS project provides support to companies in the transport and manufacturing sectors to properly address and mitigate cyberattacks and threats through free training and assessment methodologies for sector employees. Similarly, the CyberSec project brings together 15 Higher Education Institutions and 13 companies from 16 countries working on an agile, collaborative, and multi-modal training program. The European Commission's Cybersecurity Skills Academy (under the umbrella of which was recently launched the Industry-Academia Network) aims to address the growing cybersecurity skills and talent shortage in Europe. The European Cybersecurity Competence Centre (ECCC) is driving efforts in collaboration with the Network of National Coordination Centres (NCCs) across Member States. The work of ENISA, the European Union Cybersecurity Agency (referenced plenty of times further up in this brief) is key to strengthening cybersecurity across the EU, and in promoting cybersecurity skills development and making available cybersecurity tools and resources for organisations, employees, and citizens alike. ENISA's ECSF, the European Cybersecurity Skills Framework is another hands-on tool that supports the identification and articulation of tasks, competences, skills and knowledge associated with the roles of European cybersecurity professionals. It is also the EU's reference point for defining and assessing relevant skills. The European Cybersecurity Skills Challenge (ECSC) takes place each October and sees young talents compete in teams, working on cyber-related challenges and tasks.

These initiatives, together with many more, aim to strengthen cybersecurity capabilities and enhance competitiveness. Developing cyber skills remains a central and strategic priority for the EU and its Member States, and a key pillar of the EU Cybersecurity Strategy.

Conclusion

Developing cybersecurity skills and cultivating awareness of cyber threats is not merely a technical or compliance issue—it's a strategic imperative that should be embedded within the core operations and value chain of an organisation. To be effective, these initiatives must align with the organisation's specific business objectives, asset priorities, and threat environment. By integrating cybersecurity into strategic, operational, tactical and technical levels, organisations can build a truly resilient culture that not only defends against threats but also supports growth, continuity, and value creation.

Ultimately, cybersecurity skill-building is an ongoing process that requires risk-driven prioritisation, continuous management involvement, and adaptive learning strategies. When well-executed, it enhances an organisation's capacity to respond to real-world threats intelligently and efficiently, ensuring both its people and assets are prepared and protected.

The main key takeaways that need to be included are listed as follows:

- **Business-Driven Cybersecurity:** Cybersecurity skill development must reflect and support the organisation's business goals and the protection of both tangible and intangible assets.
- **Multi-Level Integration**: Effective cybersecurity requires coordination across strategic, tactical, operational, and technical domains, ensuring consistent protection and awareness at every organisational level.
- **Time as a Critical Asset:** Cybersecurity training must be efficient and purposeful, respecting the time constraints of the organisation while addressing essential security needs.
- **Threat-Aware Training:** Programs should be informed by real, evolving threats and attack vectors, grounded in solid cyber threat intelligence.

- **Tailored and Prioritised Approach:** Training and awareness efforts must be customized based on risk exposure, functional roles, and business-critical assets, prioritizing the most impactful areas.
- **Human Factor is Central:** Personnel across all organisational levels play a crucial role in the cybersecurity value chain; thus, engagement, awareness, and role-specific skills are vital.
- **Metrics-Driven Monitoring:** Key Performance Indicators (KPIs), Key Goal Indicators (KGIs), and Key Risk Indicators (KRIs) are essential for evaluating and improving training effectiveness.
- **Continuous Management Involvement:** Senior leadership must be actively engaged throughout the process to ensure alignment, resource support, and sustained organisational commitment.

By adopting a comprehensive, intelligence-led, and business-aligned approach, organisations can foster a cybersecurity-aware culture that is capable of adapting to today's complex and dynamic threat landscape.

The ultimate goal of the training is to upscale the existing capacity and capability of the work force in a time effect schema tailored to the business objectives of the organisation as part of the overall security governance and the security architecture. Another key objective is to enhance organisational security readiness through an effective incident response framework, positioning employees as a critical line of defence and a proactive countermeasure against current and emerging cyber threats.

References

European Commission, 2020. Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020JC0018.

European Commission, 2024. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). Available at: https://eur-lex.europa.eu/eli/reg/2024/1689/oj

European Parliament, 2022. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive, consolidated text). Available at: http://data.europa.eu/eli/dir/2022/2555/2022-12-27.

European Union Agency for Cybersecurity (ENISA). *European Cybersecurity Skills Framework (ECSF)*. Available at:https://www.enisa.europa.eu/topics/skills-and-competences/skills-development/european-cybersecurity-skills-framework-ecsf.

European Union Agency for Cybersecurity (ENISA), 2017. *Threat Landscape Report*. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017.

European Union Agency for Cybersecurity (ENISA), 2024. *Threat Landscape Report*. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

Von Solms R, Von Solms B., 2006. ‘Information security governance: A model based on the Direct-Control cycle‘ in *Computers & Security*, Vol 25:6. (pp. 408 – 412).