Developing a Comprehensive Model for Digital Lifelong Learning Using Cyber Resilience Framework

Costel CIUCHI, PhD
Associated Professor at University POLITEHNICA of Bucharest
Information Technology and Digitalization Directorate, General Secretariat of the Government
costel.ciuchi@gov.ro

Abstract

Ensuring a secure environment through the use of information systems are mandatory requirements of today's society, practically it become an intense and ongoing concern in relation to possible risks and threats. The development of organizations is conditioned by the use of information systems, which gain vital importance over time and become the "engine" of daily activity. Also, in addition to the fact that information systems meet administrative and operational needs, they have gradually gained a significant share at all levels of the organization, up to the strategic and decision-making level. The working flows model must include new approaches, starting from the technological levels to managerial levels including most important layer of an organization: human resources. User's education and cybersecurity management knowledge represent an important part of ensuring the real organization's data and influenced managerial decisions. Technological threats and vulnerabilities can compromise decisional process starting from the early stages. With all the latest security technology implemented, a system will become cyber resilient if will take in consideration the 3 dimensions - human resources, processes, and technology. To achieve this goals, new approaches in cyber security education is needed. The diversity of technologies and accelerated developments of information technology in all domains need to be supported by a complex educational environment who must meet the actual society requirements.

Index terms: cyber resilience, cybersecurity, education, learning framework, resilience

1. Introduction

Nowadays, the big question it is not if your network will be attacked, but when it will be attacked? And the real question is how quickly can you respond to the threat and recover? The diversity of vulnerabilities and threats, doubled by the complexity of the attack vectors reinforce the need for cooperation in cyber education, awareness, and professional training.

To diversify the education and training process comes from the need to acquire abilities and skills in cybersecurity which is a consequence of a constantly dynamic global competition and the growing demand for a better-skilled workforce adapted to accelerated technological changes.

There are new domains and directions in cybersecurity that need to update the educational and training process, close to realities from generated by complex vulnerabilities and threats. Exploring new methods and methodologies is expected in the next period.

First step is to enhance a collaborations ecosystem between academia, the private sector, and public administration to develop cooperation platforms for exchange ideas and educational programs in field of cybersecurity.

2. Education, awareness and professional training process in the field of cybersecurity

Achieving goals in cybersecurity requires updating and developing new models and frameworks for enhance skills to all employees an organization, both horizontally and vertically concerning all areas of activity are needed.

The growing demand for a better-skilled workforce adapted to accelerated technological changes and to threats or vulnerabilities from cyberspace need to be supported by adaptive educational, awareness and professional training processes.

The current status of educational process in the field of cybersecurity remarks two approaches the field from different perspectives, such as NICE Cybersecurity Workforce Framework and European Cybersecurity Skills Framework.

2.1. Cyber-Resilience Framework

Staring from the process of the design, technical systems must have a set of characteristics like dependability (availability, reliability, maintainability, safety) and security. To became resilient, there were identified four essential specific features:

- **monitor** critical developments;
- **respond** to what is happening;
- **anticipate** threats and opportunities;
- **learn from** experience - from success, but especially from **failures**.

Cyber-resilience represents a framework that is designed to help organizations withstand attacks. It is an iterative process that provides the ways of recovery from an attack and allows a constant vigilance across the organization.

Once bypassed, traditional defenses become useless, but cyber-resilience integrates security into the core of the business itself, allowing for the resilience components to be present in all areas of the business. To build a cyber-resilience capability, organizations must focus on shortening the life-cycle stages between defense and detection and response and recovery.

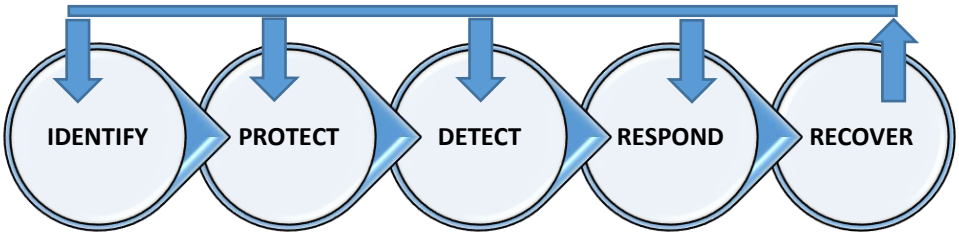

Fig. 1. Cyber-Resilience Framework [1]

To ensure resilience to an organizational ecosystem an important approach is to take in considerations all the dimension's, human resources, processes, and technology, with are involved in business model not only the technological part.

An important aspect related to cyber resilience culture in an organization, based on every component stage of resilience, is to develop and to build for the human resources and workforce an educational and continuous professional training strategy.

2.2. NICE Cybersecurity Workforce Framework

National Institute of Standards and Technology (NIST) developed a framework under The National Initiative for Cybersecurity Education (NICE) [2], Cybersecurity Workforce Framework

(NICE Framework) with the purpose to unify resources that establishes a unitary taxonomy and lexicon to describe processes from the cybersecurity domain. Also, connecting essential activities and associated tasks requires new skills and competences for the specialists, regardless of the particularity of the cybersecurity subdomain in which it operates. Modeling essential activities and associated tasks requires the development of the necessary steps to be taken in ensuring cybersecurity.

The NICE framework consists of interconnected components, the main grouping of common cybersecurity functions (categories - 7), distinct fields associated with activities (specialized area - 33) and detailed working groups which include the specific knowledge, expertise, abilities, and skills needed to perform tasks in a working role (working roles - 52).

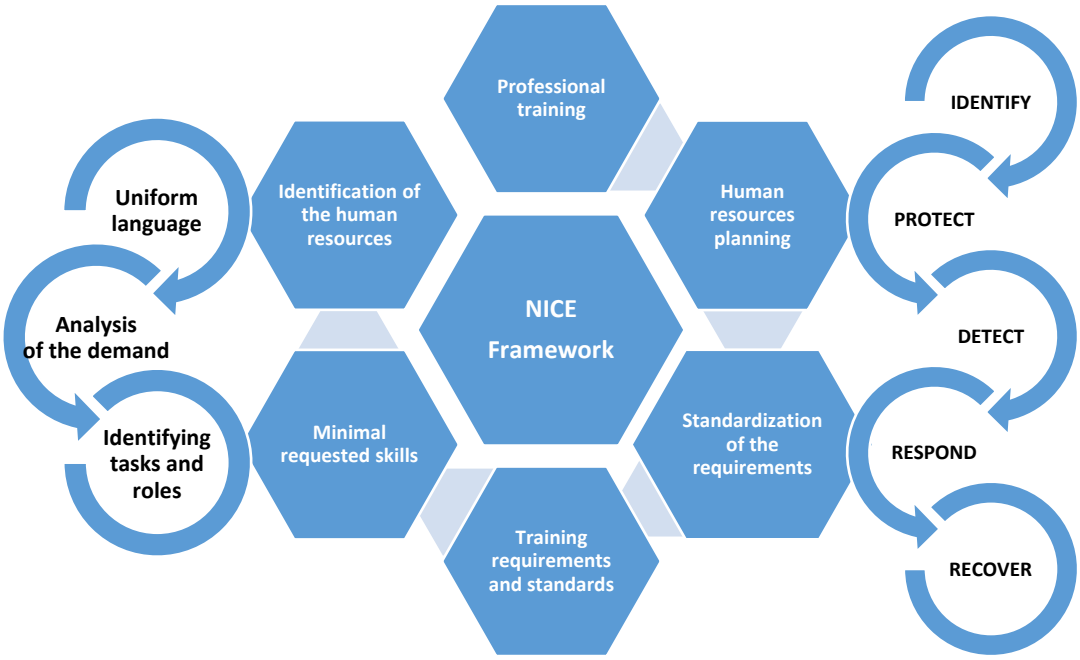

Fig. 2. Training and development model of skills [2]

In a continuous transformation domain, cybersecurity field needs experts with a complex and dynamic portfolio of expertise to face and execute essential cybersecurity actions for an organization.

Table 1. Mapping cyber resilience stages and NICE Framework categories

NICE Categories	*Resilience Stages*
Analyze (AN)	**Identify**
Collect and Operate (CO)	
Investigate (IN)	**Protect**
Operate and Maintain (OM)	**Detect**
Oversee and Govern (OV)	**Respond**
Protect and Defend (PR)	
Securely Provision (SP)	**Recover**

The main directions of common cybersecurity categories include the basic principles of resilience and represent a starting point for the developing a complete educational ecosystem.

2.3. EU Framework for Digital Education and Cybersecurity

European Union launch some initiatives to ensure a common understanding of the roles, skills, abilities, and knowledge used by and for employees, employers, and training providers in all EU member states to address the cybersecurity skills shortage.

The Digital Education Action Plan (2021-2027) [3] consist in a set of 13 action and is structured around two strategic priorities:

- promoting the development of a high-performance digital education ecosystem;
- improving skills and competencies for digital transformation.

The action plan is a result from challenges and opportunities of the COVID-19 pandemic, which has led to the unprecedented use of technology for education and training purposes.

The need to develop programs and mid-term plans, appear as a necessity especially in cybersecurity field, where Cybersecurity Act [4] granted ENISA new tasks to set up and maintain the European cybersecurity certification framework.

Also, strategy [5] is about reinforcing the presence on the technology, making up for the deficiencies of cybersecurity skills by enhancing cyber awareness, it aims to strengthen cyber diplomacy and cyber defence and to promotes standardization.

The development of a European Cybersecurity Skills Framework that would take into account the needs of the EU and each one of its Member States is considered an essential step towards Europe's digital future. Also, a common understanding of the roles, competencies, skills and knowledge used by and for individuals, employers and training providers across the EU Member States, in order to address the cybersecurity skills shortage is needed.

The European Cybersecurity Skills Framework is a result of joint work of ENISA and a relevant Ad Hoc Working Group on the European Cybersecurity Skills Framework [6]. The Group was formed in July 2020, following an ENISA public call for the creation of a multi-disciplinary group of experts that would promote harmonization in the ecosystem of cybersecurity education, training, and workforce development and develop a common European dialect for cybersecurity skills [6].

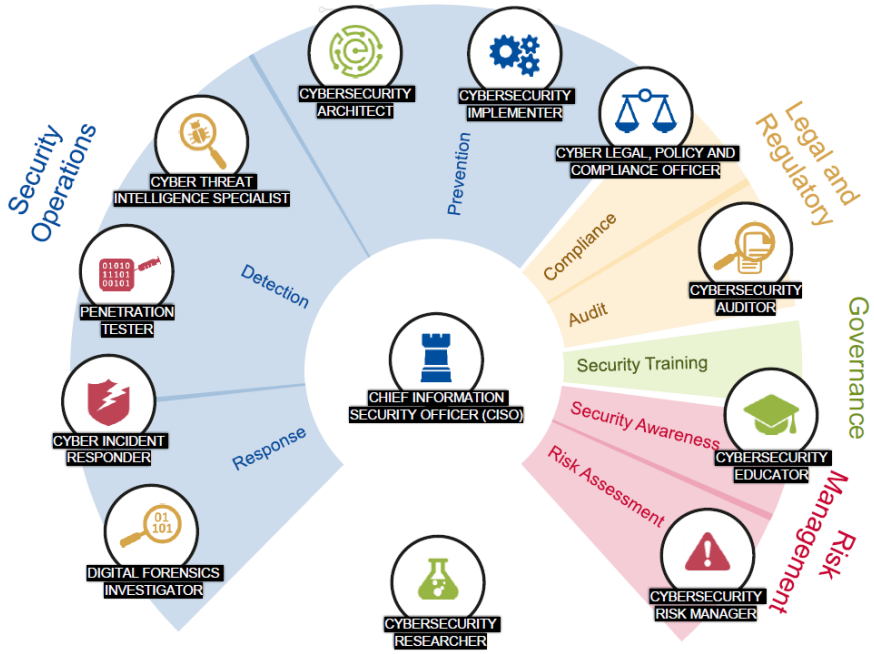

Fig. 3. CISO Mind Map - European Cybersecurity Skills Framework [7]

European Cybersecurity Skills Framework - is the European model that aims to facilitate the recognition of cybersecurity skills and become support for training programs in the field.

In this proposal, 12 relevant profiles in the field were selected to which unitary elements (dimensions) were associated, among which I mention: mission, deliverables, main tasks, main skills, key knowledge and e-Skills.

The main goal of this approach [7] is to create a robust, easy to use, expandable, neutral accessible, interoperable framework who will:

- Create a common understanding of the roles, competencies, skills and knowledge;
- Facilitate cybersecurity skills recognition;
- Support the design of cybersecurity related training programs.

3. Resilient model for learning process in cybersecurity

Improving education and research, represent key to achieving the overall objectives of cybersecurity policy and developing a trained workforce. Research and education approaches will only be effective if they include the multilateral and multidisciplinary nature of cybersecurity as a fundamental and ubiquitous element in culture, approaches, processes, systems, and technical infrastructures [8].

From the human resources perspectives, the approach of resilience requires the coordination of the main educational flows: learning / training / certification / assessment (EDU.LTC-A Cycle).

Fig. 4. EDU.LTC-A Cycle - Modelling the learning process

Relevant and quality skills and competencies are elements that need to be developed in accordance with the level of criticality associated with threats.

The need to update the educational mechanisms that can be adopted in order to develop complex models can be achieved considering the development of **key (technical) competencies** and **cross-cutting competencies** [9].

Table 2. Cross-cutting competencies [9]

	CROSS-CUTTING COMPETENCIES
ADEQUACIES (QUALIFICATIONS)	EVALUATION, COMMUNICATION, ANALYSIS, INVESTIGATION
ESSENTIAL SKILLS	INTUITION, CREATIVITY, ADAPTABILITY, CONTINUOUS LEARNING

The complexity of threats and cybercrime scams need to develop skills not only for professionals. Education for all users that use a system must be one of the priorities for critical infrastructure.

They must have competences and skills to identify and to report anomalies and all the intrusion attempts from their perspectives, in order to raise the level of security. In order to achieve this objective, a close cooperation is need between managers, developers, administrators and users.

Based on support of ENISA Ad-Hoc Working Group on Cybersecurity Threat Landscapes (CTL) [10], a report regarding Cybersecurity Threat Landscape for 2020-2021 (released in October 2021) were identified main threats, major trends observed with respect to threats, threat actors and attack techniques, and also were described relevant mitigation measures.

There are few important aspects that ENISA Cybersecurity Threat Landscape Report [11] reveals like:

- preferred target of attackers was public and government sector;
- most of the breaches in 2020 were caused by errors and system misconfigurations;
- highlights a spike in non-malicious incidents, human errors.

A different approach is needed to be settle for education process, professional training, awareness, and certification in cybersecurity. The proposed educational model has as main objectives the development of specific competencies and transversal skills considering the main attributes associated with resilience.

The development of educational processes in close connection with the cyber resilience framework will ensure the achievement of cyber resilience objectives and the achievement of a secure environment in accordance with the basic requirements associated with the field of cyber security.

Modeling educational flows based on the basic attributes associated with the cyber resilience framework (Identify, Protect, Detect, Respond, Recover) will ensure high security for technical systems, workflows and users. Also, the elements necessary to be improved will be highlighted, both from the point of view of human resource preparation and from the perspective of the competencies necessary to be developed:

- a common understanding of the roles, competencies, skills and knowledge used by and for individuals, employers and training providers;
- developing skills recognition framework and training programs in cybersecurity;
- building and sustain a professional cybersecurity workforce.

4. Conclusions

Cyber-attacks have been experiencing explosive diversification lately, some of which can be classified as global epidemics due to the high speed of spreading in the virtual environment. The threats to the information systems are characterized by an increased dynamics and a global character, making them difficult to identify and counteract.

Although there are numerous and better performing methods of protection, ensuring information security in the cyber environment can't be achieved only by technical measures, being mainly a human problem. Security incidents are frequently generated by an inadequate organization of security policies and less because of a security system failure. In this context, it is necessary to develop strategies on cybersecurity by defining policies in this respect and campaigns to prevent and combat cybercrime at national level [8].

Research and education in the field of cybersecurity must be priorities of public policies. Strengthening information security research, improving education and developing trained workforce are essential to achieving the overall cybersecurity policy objectives.

International cooperation plays a key role in this area, as cybersecurity challenges go beyond boundaries, extending to global interconnected systems. Collaboration with European and International entities is absolutely necessary, whether it is educational establishments, research centers, private companies or government institutions. Cooperation between institutions, organizations and the cybersecurity community can be useful in finding and fixing vulnerabilities. A proven cooperation mechanism in this regard is the coordinated disclosure of vulnerabilities [8].

Adoption of coherent public policies at Members State level on coordinated vulnerability disclosure and coordinated cross-sectoral action / trans-sectoral cooperation mechanisms will provide

the necessary ecosystem to ensure security in the community. The opening of communication channels, the creation of working groups and public consultation, the involvement of civil society and the public-private partnership are key directions that public policies should focus on.

This article aims to highlight avenues for an education model and an international collaboration to effectively combat threats and cybercrime. Using new approaches and methodologies to assist organizations and authorities to provide a platform for exchange of best practices, share resources for educational process in cybersecurity.

The need to respond to cybercrime and to raise awareness among relevant stakeholders and specially for the public on related matters, represent a key element that make from education domain a central pillar to any cybersecurity strategies [12].

Concluding, the adoption of comprehensive and up-to-date cybersecurity legislation to support the development of education capabilities should be a national priority. Ensuring a secure cyberspace is the responsibility of both the state and the competent authorities, the private sector and civil society. For the development of the cybersecurity culture, the most important levers are education and research, public-private partnerships and cooperation mechanisms at European level.

References

[1]. F. Dickson, P. Goodwin, Five Key Technologies for Enabling a Cyber-Resilience Framework, White Paper, International Data Corporation (IDC), Sponsored by: IBM, October 2020, Available: https://www.ibm.com/downloads/cas/YBDGKDXO.

[2]. National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NICE Framework), NIST Special Publication 800-181, National Institute of Standards and Technology, July 28, 2020, Available: https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework.

[3]. Digital Education Action Plan (2021-2027), European Commission, COM (2020) 624, Available: https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_en.

[4]. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act, Official Journal L 151 15 (2019). Available: http://data.europa.eu/eli/reg/2019/881/oj.

[5]. European Commission (2020b) The EU's cybersecurity strategy for the digital decade. Available: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2020:18:FIN.

[6]. Ad-Hoc Working Group on the European Cybersecurity Skills Framework, Available: https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework/adhoc_wg_calls.

[7]. European Cybersecurity Skills Framework, Webinar, Available: https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework/webinar-presentations.zip.

[8]. I.C. MIHAI, C. CIUCHI, G. PETRICĂ, Current challenges in the field of cybersecurity - the impact and Romania's contribution to the field, The European Institute of Romania. - Bucharest, 2018, Available: http://ier.gov.ro/wp-content/uploads/2018/10/SPOS_2017_Study_4_FINAL.pdf.

[9]. C. CIUCHI, Building a Resilient Ecosystem for Cybersecurity in Education, Cybersecurity - Challenges and Perspectives in Education, I.C. MIHAI, C. CIUCHI, G. PETRICĂ (editors), pp. 141-152, ISBN: 978-3-940237-26-2, DOI:10.19107/CYBERSEC-EDU. 2020.EN, Academica Greifswald, Rostock, Germany, 2020.

[10]. Ad-Hoc Working Group on Cyber Threat Landscapes, Available: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/ad-hoc-working-group-cyber-threat-landscapes.

[11]. ENISA Threat Landscape 2021, Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021.

[12]. Considerations on Challenges and Future Directions in Cybersecurity, I.C. Mihai, C. Ciuchi, G. Petrică (coord.), eISBN 978-606-11-7005-0, ISBN 978-606-11-7004-3, Sitech, 2019, Available: https://www.arasec.ro/documente/CybersecurityRO2019.pdf.