Cybersecurity education in Romania - competitive advantage in the EU market

Ioana-Cristina VASILOIU

National Institute for Research & Development in Informatics – ICI Bucharest
8-10 Maresal Averescu Av., Bucharest, Romania

Bucharest University of Economic Studies
6 Piata Romana, 1st district, Bucharest, Romania

ioana.vasiloiu[at]ici.ro; ioana.vasiloiu[at]csie.ase.ro

Abstract: *Modern information and communication technologies have experienced significant development in recent years, with a major impact on every aspect of life: social, political, economic, and cultural. The development of cybercrime is also based on the revolutionary growth of technology. Education and courses provided at a national level are essential to prevent cyber attacks. Cybersecurity awareness and the need for cybersecurity specialists make a significant competitive advantage in the EU market. Therefore, it is crucial to know who the primary providers of cybersecurity education in Romania are and if there is room for improvement. Also, it is critical to understand who is seeking to acquire knowledge in this field and how the providers approach them. Thus, this paper presents both universities and private entities which provide at least one course focused on cybersecurity Moreover, it analyses Romania's attitude in a European environment toward this field and how and when its strategy will lead to a competitive advantage in the EU market.*

Keywords: Cybersecurity, cybersecurity education, online courses, education providers.

1. Introduction

Digital transformation dominates the agenda of businesses, governments, and consumers worldwide, with increasingly substantial sums invested in cloud computing, automation, databases, and artificial intelligence (AI) technologies in recent years to facilitate work and enhance the customer experience. It applies to medical emergencies, climate change, population ageing, or other future challenges because digital technologies represent the means of progress, enabling the world to move forward.

https://doi.org/10.58503/icvl-v17y202225

The increasing use of the internet and cyber-based technologies has resulted from the fast expansion of information and communications technology (ICT) and the global digital transformation (Eriksson & Giacomello, 2022).

Nevertheless, accelerated digitalisation also brings challenges in terms of cybersecurity (Fischer-Hübner et al., 2021). Threats of this nature are increasingly numerous, and the risks are growing, which is why combating cybercrime requires collective societal responsibility (Ho et al., 2022) and tremendous coordination of forces at all levels. At the same time, people and organisations must use all the tools at their disposal – legal and technical measures, capacity building, and cooperation – to connect with each other and build trust.

The digital world has become an integral part of people's lives. All types of organisations, such as medical, financial, and educational institutions, use it to function effectively. Organisations use it to collect, process, store, and share large amounts of digital information. As more and more digital information is collected and shared, protecting this data becomes even more critical for national security and economic stability. And the tensions between data privacy, security, competition, and stability will continue to play out in the increasingly integrated global digital economy (Haksar et al., 2021).

Cybersecurity is described as the conjunction of technologies, individuals, systems, and functions working together to protect companies, networks, and people from digital theft, unauthorised access, attacks, damage, or disruptions in services (Bada et al., 2015). It is an ongoing effort to protect network systems and data from unauthorised use or attack. Protecting identity, data, and electronic devices is necessary. For organisations, the responsibility is divided by each employee to protect the entity's reputation, data, and customers. For states, when it comes to national security, the safety and well-being of citizens are at stake.

People spend more and more time online, and actions in this environment can affect their lives (European Parliament, 2020). Offline identity is who friends and family interact with daily at home, school, or work. They know personal information such as name, age, or address. Online identity is about who people are in cyberspace. Online identity is about how individuals present themselves to others online. Their online identity must provide limited information about them.

The necessity for education and training in this field prepares an organisation or individual confronted with an ever-changing security environment and the exponential growth of new IT & C technologies. Thus, Romania needs specialised courses in cybersecurity, which can always be a competitive advantage in the EU market.

The EU’s actions to upskill the workforce, develop cybersecurity talents and invest in research and innovation are essential to protecting against cyber threats. The new cybersecurity strategy seeks to protect an international and open Internet while simultaneously providing safeguards not just to ensure security but also to protect European values and the fundamental rights of the citizen (European Commission, 2020).

The Revised Digital Education Action Plan aims to raise cybersecurity awareness both among individuals, focusing on children and young people, and organisations, particularly SMEs. Another objective is to promote women's participation in science, technology, engineering, and mathematics education and ICT jobs, upskilling, and reskilling in digital skills (European Commission, 2020).

Through the Digital Education Plan, the European Commission establishes two strategic priorities:

1. Fostering the development of a high-performing digital education ecosystem.

2. Enhancing digital skills and competences for the digital transformation.

Thus, Romania needs to ensure that there are enough highly-skilled specialists in cybersecurity ready to support and lead solutions to existing and potential challenges related to this field. But how well is Romania doing regarding cybersecurity? Are there sufficient universities educating students in this field? Or is cybersecurity an overlooked area?

2. What is cybersecurity

Cybersecurity is defined by the International Telecommunication Union (ITU) as „the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user's assets" (ITU, 2008).

It refers to the way information, devices, and digital assets (personal data, accounts, files, photos, and even money) are protected.

People, small businesses, large companies, and public administration depend on IT systems constantly. These systems are increasingly complex, including a range of services interconnecting new and older elements.

Thus, numerous potential security vulnerabilities occur that did not exist before the emergence of the digital society. Cybersecurity is particularly significant, including how the elements of a computer system are protected against cyber attackers, who could access and use them for criminal purposes.

For individuals, cybersecurity attacks can lead to identity theft and identity extortion attempts, which can cause severe damage to the individual's life. People need their data and personal information to be protected. For example, when people connect to an application or fill in the card data when making a payment online. If these systems, networks, and infrastructures did not have the proper protection, the filled data could reach attackers. The same applies to organisations, which store enormous amounts of data, much of which is sensitive information.

According to Marsh Risk Resilience Report (Marsh, 2021), even if 45% of the organisations rated cyber risk as the most critical threat, only 18% of them state that they are highly prepared for it.

Moreover, within the tenth edition of the ENISA Threat Landscape report, there were identified the prime threats: ransomware, malware, social engineering, threats against data, threats against availability, Denial of Service, threats against availability: Internet threats, Disinformation – misinformation, and supply-chain attacks (ENISA, 2022).

Therefore, it is important to understand the **CIA triad, confidentiality, integrity, and availability,** as a guide to an entity's information security.

Confidentiality provides data protection by limiting access and encrypting authentication. Company policies should limit access to information to authorised personnel and ensure that only authorised individuals view this data. Data can be divided according to the information's level of security or sensitivity. For example, a Java developer should only have access to the personal information of some employees. In addition, employees should receive training to understand best practices for securing sensitive information to protect themselves and the company from attacks. Privacy protection methods include:

- Data encryption.
- User ID and password.
- Two-factor authentication.
- Reduced exposure of sensitive information.

Integrity ensures that information is correct and trustworthy. Integrity is the accuracy, consistency, and reliability of data throughout its entire life cycle. Data must be unchanged during transit and not modified by unauthorised entities. Permission levels assigned to files and user access control can prevent unauthorised infiltration. Version control can be used in order to avoid accidental changes by authorised users. Backups must be available to recover corrupted data, and checksum hashing can be used to verify data integrity during transfer.

Availability guarantees that data is accessible to authorised individuals. Maintaining equipment, performing hardware repairs, updating operating systems and software, and creating backups ensure network and data availability to authorised users. Following natural or manufactured disasters, there must also be plans for rapid data recovery. Security equipment or software, such as a firewall, protects against downtime caused by denial of service (DoS) attacks. Denial of service refers to the action by which a hacker tries to overload resources so that services are unavailable to users.

3. Cybersecurity culture in Romania

LAW no. 362 of December 28, 2018, establishes the legal and institutional framework, measures, and mechanisms necessary to provide a standard high level of security of networks and IT systems and to stimulate cooperation in the field (Romanian Parliament, 2018).

In this context, Romania has developed a cybersecurity culture regarding the security of networks and IT systems, with several cybersecurity awareness campaigns in place. These campaigns are conducted by Romanian institutions

(National Cyber Security Directorate, National Institute for Research and Development in Informatics, Romanian Intelligence Service, Romanian Police), non-governmental entities (The Romanian Association for Information Security Assurance (RAISA)), professional associations (The Romanian Association of Banks) or private companies (Microsoft, Bitdefender, Orange, RDS).

The Global Risks Report 2022 states that 95% of cybersecurity issues are traced to human error (World Economic Forum, 2022). Therefore, the human-generated risk as an IT&C infrastructures operator becomes a major one. This is because the threat has continuity. It starts with training and the actual perception of obligations, complying with the job description. Thus, the cybersecurity culture must be developed before beginning professional activity.

According to the Digital Economy and Society Index (DESI) 2022, Romania ranks 27th regarding the human capital dimension. Our country encounters a deficiency of fundamental digital skills; therefore, this applies to cybersecurity too. Less than a third of citizens have at least basic skills, and only one out of ten has above-basic digital skills. However, the proportion of ICT specialists is growing steadily, as per the graph below (Figure 1. Female ICT specialists). Also, in terms of female ICT specialists, Romania is above the EU average (19.1%), with 26% of the total ICT specialists (European Commission, 2022).

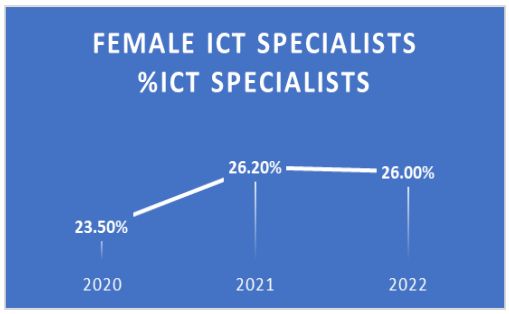

Figure 1. Female ICT Specialists

However, the future of Romania's cybersecurity culture should be brighter. Among the five objectives of strategic importance for 2022-2027, as defined within The Cyber Security Strategy of Romania, is a pragmatic public-private partnership between public administration authorities and institutions, private entities, academia, research, and citizens as a necessity since cyber-attacks target a large number and a broad spectrum of networks and computer systems (Romanian Government, 2021).

Within this objective, there are the following measures:

1. Running public awareness programs and raising the level of cyber security culture;
2. Development of educational programs in the field of cyber security;
3. Conducting professional training programs for those who carry out activities in the area of cybersecurity;

4. Developing and strengthening cybersecurity research and innovation;
5. Development of the national cybersecurity industry.

4. Cybersecurity in universities in Romania

Since technology will not stop developing, governments, businesses, organisations, and individuals are increasingly vulnerable to cybercrime. Anyone who lost money or vital information to hackers better appreciates cybersecurity experts. Therefore, cybersecurity specialists and information security analysts are essential in today's world. Thus, the need for experts to protect different entities' information is also growing.

Over eight years, Cybersecurity Ventures tracked the number of unfilled cybersecurity positions that grew by 350 percent, from one million in 2013 to 3.5 million in 2021. The cybersecurity skills gap settles for the first time in a decade. At the same time, they predicted the same number of jobs (3.5 million) in 2025 (Cybersecurity Ventures, 2022).

Nowadays, different programs and training courses are available, but only some graduates become cybersecurity experts after just 14 modules. This is why universities have adjusted their curriculum, in order to meet workforce needs.

Academic institutions have distinct approaches to cybersecurity education. Some universities are focused on specialising early, developing bachelor's courses. Others deliver master's programs and postgraduate courses, considering the need for a computer science background.

In this context, I conducted an analysis of the current state of the cybersecurity education provided by universities in Romania, from the perspective of bachelor's courses, master's programs and postgraduate courses.

During my research, I found universities that provide cybersecurity education all around Romania (Figure 2. Romania Cybersecurity Education Providers Map). Thus, there are **16 cities** where universities provide at least a security of information system course. In total, **27 universities** offer **14 master's programs** and **nine postgraduate courses**. Moreover, Ferdinand I Military Technical Academy has the Faculty of Information Systems and Cyber Security.

Figure 2. Romania Cybersecurity Education Providers Map

The universities' steps toward cybersecurity education should be taken into account. But there is also a need for a strategy to develop a unity of efforts in order to create a skilled workforce in this field.

Table 1 below shows the 27 universities and the various programs and courses they offer in order to educate students in Romania. Some universities only provide courses for different education levels – 15, but the other 13 provide entire programs (bachelor or master). The courses range from applications in the maritime area to cyber defence, e-business security, and data security in the www. Furthermore, the most common course is the Security of Information Systems, similar to the essential introduction to cybersecurity.

Table 1. Cybersecurity education providers in Romania

University	**Education level**	**Programs/courses**
Bucharest University of Economic Studies	Master	Program: IT&C Security Master - Cyber Security
Politehnica University of Bucharest	Bachelor, Master	Programs: Advanced Cybersecurity, Security of complex computer networks; Courses: Cybersecurity introduction, Cryptography introduction, Computer, and Network Security, Security of Information Systems
University of Bucharest	Bachelor, Master	Program: Security & Applied Logic; Course: Security of Information Systems
Ferdinand I Military Technical Academy	Bachelor, Postgraduate	Faculty of Information Systems and Cyber Security, Postgraduate courses: Cyber defense technologies, Cyber defense management, Planning cyber defense activities, Digital investigations
Technical University of Construction Bucharest	Bachelor	Course: Systems engineering
Titu Maiorescu University	Master	Program: Security of information systems and information networks
Spiru Haret University	Bachelor Master	Faculty of Engineering and Informatics, Course: Information Systems Security Modern Technologies in Information Systems Engineering (Master), Courses: DevSecOps Methodologies, Computer Networks Security, IT Security Management
Constanța Maritime University	Master	Courses: Cyber Security and Risk Management, Maritime Cyber Security and Autonomous Operations, Management Induction of Maritime Cyber Security, Cyber Warfare and Maritime Risks, Global Cyber Capabilities and Trends, Maritime Cybersecurity Law and Policy, Managing Maritime Cybersecurity Operations, Cyber

		Practitioner in Maritime Cybersecurity Simulation Lab, Risk Analysis and Compliance in Maritime Cybersecurity, Information Assurance
Ovidius University of Constanța	Master	Program: Cyber Security and Machine Learning
„Dunărea de Jos" University of Galați	Master	Program: Combating Cybercrime
Vasile Alecsandri University of Bacău	Postgraduate	Course: Cybersecurity
Technical University "Gheorghe Asachi" Iași	Master	Program: Cyberspace Security
Alexandru Ioan Cuza University of Iași	Bachelor	Course: Security of Information Systems
Ștefan cel Mare University of Suceava	Postgraduate	Courses: Fundamentals of Cyber Security, Information Systems Security, Cyber Security Incident Management
Petroleum-Gas University of Ploiești	Bachelor	Courses: Data security, Cryptography and information security
Henri Coandă Air Force Academy	Bachelor	Course: Cybersecurity
Transilvania University of Brașov	Master	Program: Cyber Security
University of Pitești	Master	Program: Advanced Techniques for Information Processing, Information security
University of Craiova	Bachelor	Courses: E-Business Security and Risk Management, Information Security
„Constantin Brâncuși" University of Târgu Jiu	Bachelor	Courses: Data security in the WWW, Data security in a network
Lucian Blaga University of Sibiu	Bachelor	Course: Information Systems Security
Technical University of Cluj-Napoca	Master	Program: Information and Computing System Security
Babeș-Bolyai University	Postgraduate	Course: Information Systems Security
Polytechnic University of Timișoara	Master	Program: Security of Information and Cyber Systems
West University of Timișoara	Bachelor, Master	Courses: Information Systems Auditing, Cryptography, Program: Cybersecurity
Vasile Goldiș" Western University of Arad	Bachelor	Course: Security of Information Systems
University of Oradea	Bachelor	Course: Security of Information Systems
Spiru Haret University	Postgraduate	Course: The audit and security of IT systems

We can conclude from Table 1 that in the bigger cities, where the cyber sector is more developed, the need for specialising students in cybersecurity is met

more than in the small ones. Therefore, the most important cities in Romania also provide master's programs or even an entire faculty, as there is in Bucharest. Meanwhile, the small towns and the smaller universities still understand the need for specialists in this field, and they have started to provide students with introductory or postgraduate courses.

In the future, we can also expect smaller universities to provide master's programs or even an entire bachelor's program. Romania now knows the importance of cybersecurity specialists, so it has started to grow its own. Soon, they will be the professionals every entity is searching for.

Conducting this study was relevant to cybersecurity education in Romania, which still needs a curriculum and an integrated approach. Therefore, government and industry should closely collaborate with the universities to demand skills that future experts need to face a cyber-attack. Collaboration is required on all ends in order to create a competitive advantage for Romania in the EU market.

6. Cybersecurity courses in Romania

Cybersecurity is one of the most crucial matters impacting governments, organisations, companies, and customers. Every year, the number of cyberattacks, malware, data and identity theft, ransomware, and fraud continue to increase. Cybersecurity attacks are still expanding not only in the matter of vectors and numbers but also regarding their impact (ENISA, 2022). The positive side is that more people are curious to discover how to defend themselves and their organisations from cybercrime.

As an alternative to university programs, the shortest and easiest way to achieve cybersecurity competencies is through various courses on the market. Anyone can easily find these courses online by a quick search on every search engine.

For instance, using Google as a search engine, I have found **24 courses**, starting from one hour (after the war in Ukraine, Ascendia offered a free course for Romania and Moldova) to 120 hour-course. The price for these courses ranges from 50 euros to 2350 euros. The primary providers of this kind of education are the National Institute for Research and Development in Informatics, Info Academy Bucharest, CISCO, Ciseo, Teachbit.ro, Cyberstart, Factory 4.0, Computerland.ro, ITtrainings.ro, Skillab.ro, IT Level, DoIt Academy.

Each course has its requirements, syllabus, price, and target audience. Still, regardless of whether people want to enhance their cybersecurity knowledge for personal, professional, or academic purposes, they can find a suitable option online. Unfortunately, there are no standards regarding these courses, and not all providers can offer a diploma accredited by the National Qualifications Authority.

7. Conclusions

Cybersecurity is a constant effort to protect network systems and data from cyberattacks, malware, data and identity theft, ransomware, and fraud. Since people use technology increasingly, the demand for education in this field has grown exponentially.

Education and training in cybersecurity are essential for organisations and individuals facing various cyberattacks. Therefore, Romania is taking action to have specialised people in cybersecurity, a competitive advantage in the EU market.

Although there are no national standards, the state of cybersecurity education in our country is evolving, having universities and private entities as providers. Students can be educated in this field at the graduate and postgraduate levels, with only some universities requiring prior education.

Analysing the Cyber Security Strategy of Romania and its objective to create a pragmatic public-private partnership establishes the framework for developing education in this field.

Raising public awareness and designing new awareness campaigns leads to a better cybersecurity culture. The educational programs in this field will also help, especially if the Government applies standards. Professional training programs for those who carry out activities in the area of cybersecurity are needed since this is an ever-changing area. Funding for research and innovation is necessary to keep pace with the emerging challenges in the cyber environment. All these aspects will help develop the national cybersecurity industry and make a difference, leading to a competitive advantage in the EU market.

The next step should be to promote the 16 cities, 27 universities, 14 **master's** programs, and nine postgraduate courses. There is excellent potential for cybersecurity education in Romania, but it still needs to be adequately advertised. Many of the universities in this research are state universities; therefore, schooling is free, unlike the other 24 courses I have found online, which need payment.

The need for cybersecurity experts will still grow in our country, even if it has settled at a global level. Thus, Romania should take advantage of all the university programs to improve its DESI rank and cybersecurity culture.

References

Bada, M., Sasse, A., Nurse, J. (2015). *Cyber Security Awareness Campaigns: Why do they fail to change behaviour?*. https://arxiv.org/ftp/arxiv/papers/ 1901/ 1901. 02672.pdf .

Cybersecurity Ventures (2022, January 19). *2022 Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics*. https://cybersecurityventures.com/ cybersecurity-almanac-2022/.

Eriksson, J., Giacomello, S. (2022). *Cyberspace in space: fragmentation, vulnerability, and uncertainty*. Cyber Security Politics. London, Routledge.

European Commission (2020, December 16). *The EU's Cybersecurity Strategy for the Digital Decade*. https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0.

European Commission (2020, September 30). *Digital Education Action Plan 2021-2027 Resetting education and training for the digital age*. https://education.ec.europa.eu/focus-topics/digital-education/action-plan.

European Commission (2022). *Romania in the Digital Economy and Society Index*. https://digital-strategy.ec.europa.eu/en/policies/desi-romania.

European Parliament (2020, May). *Potentially negative effects of internet use*. https://www.europarl.europa.eu/thinktank/en/document/EPRS_IDA(2020)641540.

European Union Agency for Cybersecurity (2022, November 3). *ENISA Threat Landscape 2022*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022.

Fischer-Hübner, S., Alcaraz, C., Ferreira, A., Fernandez-Gago, C., Lopez, J., Markatos, E., Islami, L., Akil, M. (2021). Stakeholder perspectives and requirements on cybersecurity in Europe. *Journal of Information Security and Applications.*

Ho, H., Ko, R., Mazerolle, L. (2022). Situational Crime Prevention (SCP) techniques to prevent and control cybercrimes: A focused systematic review. *Computers & Security*.

Haksar, V., Carrière-Swallow, Y., Giddings, A., Islam, E., Kao, K., Kopp, E., Quirós-Romero, G. (2021). *Toward a Global Approach to Data in the Digital Age.* https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2021/10/06/Towards-a-Global-Approach-to-Data-in-the-Digital-Age-466264.

International Telecommunication Union (2008, April 18). Series X: Data Networks, Open System Communications and Security Telecommunication Security. *Overview of cybersecurity*. https://www.itu.int/rec/T-REC-X.1205-200804-I.

Romanian Government (2022, January 3). *The Cyber Security Strategy of Romania*. https://legislatie.just.ro/Public/DetaliiDocumentAfis/250235.

Romanian Parliament, (2018). *LAW no. 362 of December 28, 2018, on ensuring a common high level of security of networks and IT systems*. https://legislatie.just.ro/Public/DetaliiDocument/209670.

World Economic Forum (2022). *The Global Risks Report 2022, 17th Edition.* https://www3.weforum.org/docs/WEF_The_G.