CYBERSECURITY AS A GOOD LIFE PATH FOR EVERYONE

Aleksandra Pyrkosz, Sabina Szymoniak

Department of Computer Science, Czestochowa University of Technology (Poland)

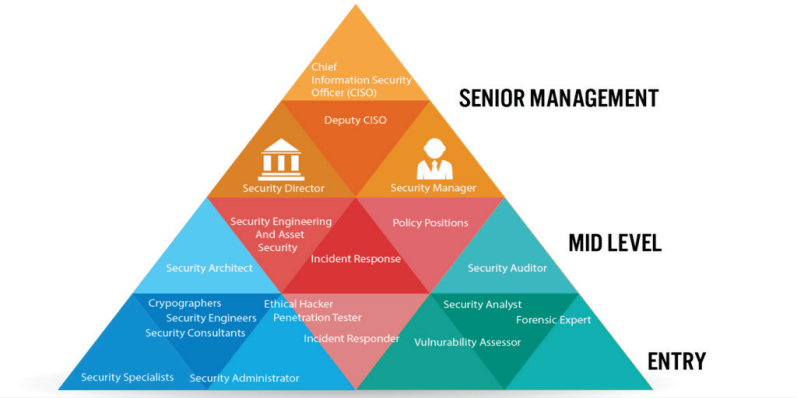
aleksandra.pyrkosz98@gmail.com; sabina.szymoniak@icis.pcz.pl

EXTENDED ABSTRACT

Cybersecurity is one of the most exciting areas of work and science. It is evident in the digital area, where almost every company, regardless of size, has an Internet connection. Access to the network offers many opportunities but also entails new challenges. One of them is the proper care of security in cyberspace.

Along with the growing importance and use of digital technologies, the number of threats that organisations must counter also increases. Cybercriminals are using more advanced attack methods, so building security is evolving and improving. The introduction of effective security practices in cyberspace is crucial for protecting information, maintaining customer trust, and maintaining the stability of the company's operation in the era of universal digitisation. Responsible for cybersecurity is a continuous process and requires constant monitoring, adapting strategies and protective measures to the changing threat landscape. This is a complicated process, but there are different ones on the market with the possibility of implementing certain facilitations while maintaining an appropriate level of safety ((Steingartner et al., 2022), (Nwankpa & Datta, 2023)). Figure 1 summarizes the cybersecurity career path and shows how different activities cybersecurity specialities perform.

Figure 1. Cybersecurity career path.



- Source: https://www.spiceworks.com/tech/it-careers-skills/articles/cybersecurity-career-path/

Moreover, cybersecurity issues make a perfect space for researchers. The computer systems exposed to cyberattacks need specially designed algorithms and techniques for security improvement. Such systems need secure communication between network nodes. Thus, researchers must propose new security protocols that will define the sequence of the steps

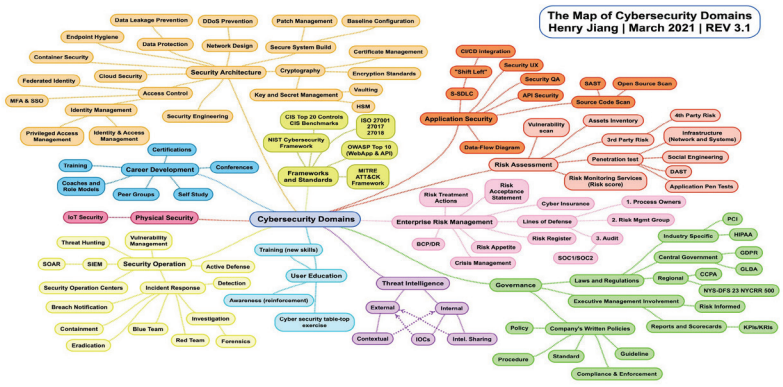
during the communications and use security techniques like encryption, timestamps, pseudonymity or hashing functions. Security protocols can be designed for cross-domain or specific solutions. Also, the security protocols should be constantly verified to check if they provide an appropriate security level ((Bartłomiejczyk et al., 2022), (Szymoniak, 2021)).

Next, computer systems need tools to check the system's vulnerabilities and Intrusion Detection and Prevention Systems (IDPS). IDPSs monitor computer networks to detect and respond to suspicious or harmful activities. They analyse network traffic and identify patterns that may indicate unauthorised access attempts, attacks, or other unwanted activity. IDPSs monitor the network traffic, analyse the packet signatures, detect anomalies and respond to the incident. These tools mainly use artificial intelligence methods and techniques in their work (Apruzzese et al., 2023). Note that IDPSs have their limitations. They may not detect new or advanced attacks whose signatures are unknown. Therefore, IDPS systems must be updated frequently and have access to up-to-date signature databases. In addition, IDPSs can generate false positives, especially in complex networks, requiring further verification and analysis by network administrators.

Moreover, the attackers are not idle. They are constantly exploring computer systems to find new doors to get in. They improve their knowledge of systems and their hacking skills. We can indicate many cyberattack types like spoofing, known session-specific temporary information or replay attacks. Also, the performed attacks can be a combination of some typical attacks. Cyber attacks can have various effects that depend on the type of attack, its purpose and how it is carried out (data stealing, sabotage, privacy violation) (Szymoniak & Kesar, 2023).

Such a variety of possible ways to improve computer system protection gives many opportunities to choose one's life path. Figure 2 shows the map of cybersecurity domains. This diagram summarises how many opportunities and interests give us in cybersecurity. This an extensive area where everyone will find their place for work and personal development.

Figure 2. Cybersecurity domains.



Source: https://www.linkedin.com/pulse/cybersecurity-domain-map-ver-30-henry-jiang

This paper's authors also choose cybersecurity as a life path. The first met with security issues during first-degree studies. The security and network topic fascinated the author to continue the Cybersecurity speciality studies. In the MA thesis, the author considered the security

simplification process in large organizations while maintaining an appropriate security level. Also, the second author works as a Cybersecurity specialist.

The second author met with security issues during PhD studies. The author considered the verification of security protocols and the impact of time on these protocols' execution. The author obtained many exciting results and presented them in many scientific articles. Also, the second author suggests new security protocols for the Internet of Things solutions in scientific work. In didactic work, this author also focuses on security issues in a broader range. The classes concern the security of computer systems in many aspects of this topic.

Both authors met as a student and a teacher, also as a graduate student and a thesis promoter, and next as co-organizers of cybersecurity events. They would like to share their experiences connected with cybersecurity and encourage everyone to choose a similar path in life.

In this paper, the authors will share their experiences connected with cybersecurity that they received during their studies and work. They will explain why they chose such a path in life and what is so interesting and exciting in cybersecurity issues. They will show their most significant achievements. Also, they will assume challenges they faced during previous activities and perspectives for development and acquiring exciting experiences offered by cybersecurity in various directions. We believe that our experiences, insights, and tips will clarify all doubts about those unsure of choosing cybersecurity.

KEYWORDS: Cybersecurity, way of life, scientific work, experiences in cybersecurity.

REFERENCES

Apruzzese, G., Laskov, P., Montes de Oca, E., Mallouli, W., Brdalo Rapa, L., Grammatopoulos, A. V., & Di Franco, F. (2023). The role of machine learning in cybersecurity. *Digital Threats: Research and Practice*, *4*(1), 1-38.

Bartłomiejczyk, M., El Fray, I., Kurkowski, M., Szymoniak, S., & Siedlecka-Lamch, O. (2022). User Authentication Protocol Based on the Location Factor for a Mobile Environment. *IEEE Access*, *10*, 16439-16455.

Nwankpa, J. K., & Datta, P. M. (2023). Remote vigilance: The roles of cyber awareness and cybersecurity policies among remote workers. *Computers & Security*, *130*, 103266.

Steingartner, W., Možnik, D., & Galinec, D. (2022, November). Disinformation Campaigns and Resilience in Hybrid Threats Conceptual Model. In *2022 IEEE 16th International Scientific Conference on Informatics (Informatics)* (pp. 287-292). IEEE.

Szymoniak, S. (2021). Amelia—a new security protocol for protection against false links. *Computer Communications*, *179*, 73-81.

Szymoniak, S., & Kesar, S. (2023). Key Agreement and Authentication Protocols in the Internet of Things: A Survey. Applied Sciences, 13(1), 404. https://doi.org/10.3390/app13010404