

ECHO Cyber-Skills Framework as a Cyber-Skills Education and Training Tool in Health and Medical Tourism

Eleonora Beltempo, Jussi Karvonen and Jyri Rajamäki

Laurea University of Applied Sciences, Finland

eleonora.beltempo@student.laurea.fi

jussi.karvonen@student.laurea.fi

jyri.rajamaki@laurea.fi

Abstract: The ECHO Horizon 2020 Project develops a European cybersecurity ecosystem. One of its assets is the ECHO Cyber-Skills Framework (ECSF). This work in progress paper aims to improve cybersecurity education and training in the healthcare industry including health and medical tourism. First, this paper finds out how ECSF will benefit the healthcare sector regarding cyber-skills and awareness in order to create a more secure information technology (IT) environment when it comes to healthcare. Based on these findings, the paper proposes a strategy to adopt ECSF in order to improve the existing state of IT security and increase worker and management awareness and understanding. Finally, the paper looks at ECSF's possibilities to be a tool for education and training in health and medical tourism.

Keywords: ECHO project, cyber-skills framework, cybersecurity, health and medical tourism

1. Introduction

ECHO (the European network of Cybersecurity centres and competence Hub for innovation and Operations) H2020 Project develops a European Cybersecurity ecosystem, to support secure cooperation and development of the European market, as well as to protect the citizens of the European Union against cyber threats and incidents (ECHO, 2021). The ECHO Cyber-Skills Framework (ECSF) aims at providing a foundation and practical guidelines for better defining the knowledge and skill gaps in the healthcare, transport and energy industries as well as for the development of cybersecurity education and training programs that address those gaps. The ECSF serves as an inventory tool, providing methodological guidelines for the design, update and development of training programs and curricula, both within the framework of the ECHO project, as well as within the scope of relevant EU initiatives, as a common reference model for capacity building (Varbanov, 2021). Figure 1 presents the main components of the ECSF.

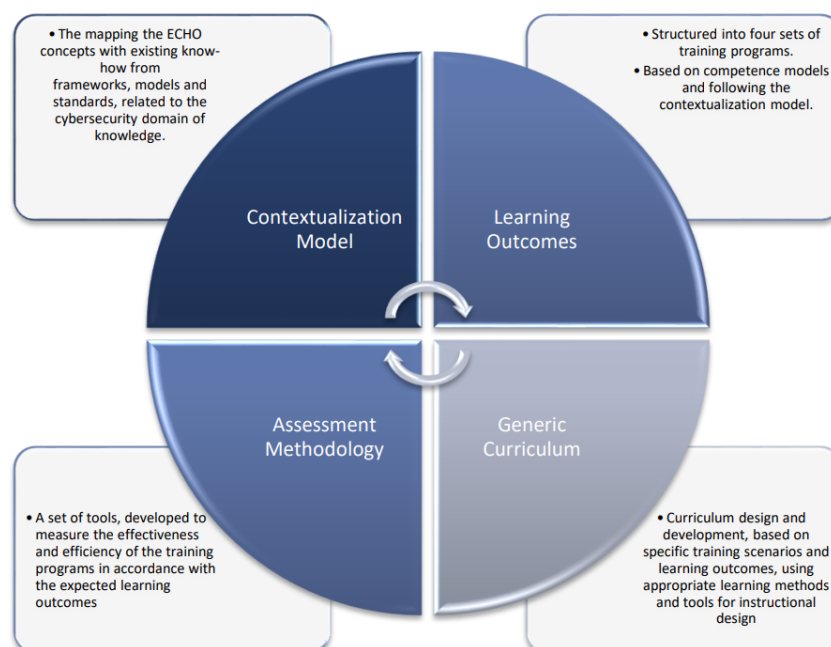


Figure 1: Main Components of the ECSF (Varbanov, 2021)

This work in progress paper finds out the possibilities of utilizing the ECSF in the healthcare industry including health and medical tourism. Although the concept of health and medical tourism is widespread, also the following terms are used when speaking of travel-based health-related activities: health tourism, medical

tourism, wellness tourism, spa tourism and medical travel (Romanova, Vetitnev & Dimanche, 2015). Figure 2 illustrates different types of health and medical tourism.

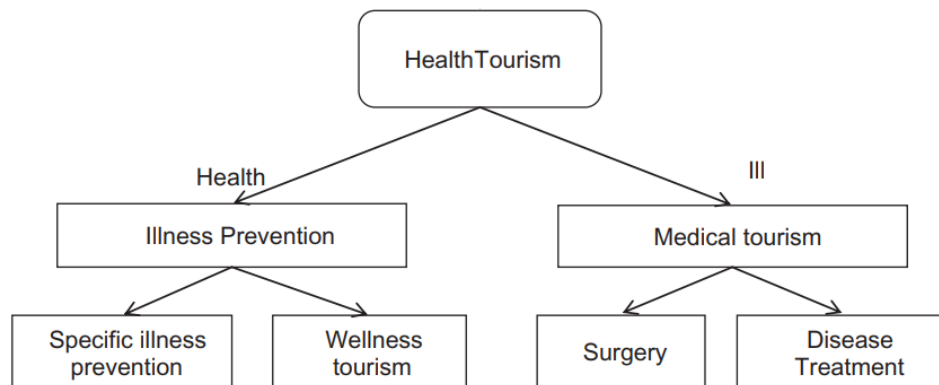


Figure 2: Typology of Health and Medical Tourism (adapted from Romanova et. al, 2015)

This study starts by answering three research questions to see how ECHO and the healthcare sector would both benefit from the possible implementation of ECSF in the healthcare sector:

- How ECHO cyber-skills framework would be beneficial for healthcare?
- What is the best way to implement the ECHO cyber-skills framework into the healthcare sector?
- How the ECHO network will benefit from this implementation.

After answering these questions, this paper combines the findings and proposes how to use ECSF in health and medical tourism.

2. Findings

From our study, we combine the information that has been gathered with the help of our research questions. We figure out what are the problems within healthcare sectors organizations, what is the best way to implement the ECSF, and how can ECHO benefit from the possible implementation of ECSF into the healthcare sector. We also search that if there are any public cyber-skills frameworks that we could possibly reference to see if there is an increase in employees' skills and awareness.

2.1 ECSF benefits for healthcare

To find out about how a cyber-skills framework could be beneficial for healthcare we must first find out about the gaps in healthcare sectors' cyber-skills, knowledge, and the state of awareness about possible threats. Secondly, we have to find out is there any kind of basic training for healthcare sectors staff regarding cyber-skills and knowledge.

The current gaps in the healthcare sector's cyber-skills, knowledge, and awareness are quite huge. According to IONOS Cloud, 37% of healthcare IT employees say their organization is at risk of security because of skills gaps in the field (Mageit, 2021). IONOS Cloud's report continues that 39% of IT professionals in the healthcare sector state that they have gaps in data protection, 25% say they are not adhering to the legislation, and 21% do not follow proper data protection measures (Mageit, 2021). These gaps and threats caused by them can lead to attackers leaking sensitive information about patients which can cause risks for health and safety, and not using critical medical services because they can be affected by unauthorized control (Varbanov, 2021).

The healthcare sector includes private and public hospitals, as well as the companies that manufacture medical devices and the pharmaceutical industry (Varbanov, 2021). The assets that ECHO Cyber-skills Framework focuses on an organizational level are the ICT assets of the company and the professionals who are responsible for making sure the ICT assets are secured. Data and information are the most important assets in a healthcare organization. From the operational technology standpoint for the healthcare sector, devices and equipment that produce data that can be exchanged in and outside the organization are key assets.

From these findings, we can determine that using ECSF would increase cyber-skills and awareness within healthcare sectors employees and lower the risk of the organizations within the sector being attacked or having a close call. Organizations can also adapt to the situations from learning from previous incidents.

2.2 Implementation of ECHO cyber-skills framework to the healthcare sector

The ECHO Multi-sector Assessment Framework (E-MAF) supports risk management decision-making, i.e. it provides a framework for understanding cyber risks and, on that basis, supports decisions on where to invest human, technological and financial resources to reduce those risks to an acceptable degree (Tagarev, Pappalardo & Stoianov, 2020). To properly implement ECSF into the healthcare sector, E-MAF has to be used to address the needs and gaps. E-MAF provides the ECSF the ways to analyze challenges and opportunities, and how to assist the development of cybersecurity technology roadmaps. Using E-MAF provides educational portfolios and training programs, and a unified definition of what skills and qualifications are needed. E-MAF includes the ECHO Security Control, which provides more specific measures divided into four different levels: Organizational, Technical, Functional, and Non-Functional. Organizational implies what the cybersecurity professionals should be able to perform, including the application of security controls, mitigation, and countermeasures. Technical implies the skills and competencies professionals must have in able to demonstrate, which includes security controls. Functional implies sector-specific knowledge the professionals must demonstrate to complete modules or programs. Non-Functional implies knowledge that carries to achieving organizational, technical, and learning objectives within the organization.

There is a lack of publicly used frameworks that focus on cyber-skills training. Hübner et al. (2019) presents the TIGER International Recommendation Framework of Core Competencies in Health Informatics 2.0. Their framework is meant to augment the scope from nursing towards a series of six other professional roles, i.e. direct patient care, health information management, executives, chief information officers, engineers and health IT specialists and researchers and educators. Another example of existing frameworks is the NICE Framework (National Institute of Standards and Technology, 2021), but it is not entirely focused on training cyber-skills and increasing awareness. It does enable cybersecurity education and training, but it is more focused on developing and supporting the workforce so they are capable of meeting cybersecurity needs. The NICE Workforce Framework for Cybersecurity is a good example when providing information about what the employees need to and how to continuously describe learner capabilities. The Frameworks benefits include, for example, enhancing employee skills, understanding needs and skills gaps in the workforce, and hiring the right people for the job, when ECSF wants to train the current employees of the organization to identify and act accordingly in situations where the risk of incidents happening regarding cybersecurity are possible.

Considering how various it is the sector regarding healthcare, a slow implementation based on staff training is essential to guarantee the success of the framework. The continuous improvement of the courses and the new tools that ECHO will develop accordingly will ensure a safe and secure environment for both the staff and the customers.

2.3 How the ECHO network will benefit from this implementation?

This study aims to find out how the ECHO network would benefit from the possible implementation of ECSF in the healthcare sector. From the possible implementation of ECSF in the healthcare sector, ECHO would form a possibly long-lasting partnership with healthcare sectors organizations. Also, from this implementation, ECHO gives themselves information and data to develop more not just with ECSF, but in many more subjects. From the implementation of ECSF into the healthcare sector, ECHO could open doors to even more sectors to produce and implement different frameworks and tools. All of these things mentioned before would let ECHO grow more itself. ECHO would also be a big part of the digitalization of the healthcare sector within the EU.

3. ECSF as a tool in education and training in health and medical tourism

The purpose of medical tourism is to go to another country for medical procedures, for example, receive treatment for a condition, or to seek enhancement. The motivation for this tourism usually is a lower cost of care or higher quality care. These activities usually are reactive to illnesses that are medically necessary or overseen by a doctor (Global Wellness Institute, 2021).

Using ECSF as a tool in education and training in health and wellness tourism would be limited to EU member states. The European Commission (2021) adopted a Recommendation on a European electronic health record exchange to make the flow of Protected Health Information (PHI) of European citizens more quickly to access and share. European Commission also mentions in the article, that ensuring citizens secure access to their data develops the transformation of health and care even more digital. Using ECSF as a part of making sure the secure access and transformation of PHI of European citizens would be a tremendous thing for both EU and ECHO. Implementing ECSF as a part of the EU member states healthcare framework would secure the availability and transformation of PHI, while also ensuring the constant training and development of cyber-skills and awareness of healthcare sectors employees.

4. Discussion

Free movement of people is one of the cornerstones of the European Union. According to the Directive on Cross-Border Healthcare, which has been implemented in the entirety of the EU since 2013 for European citizens, no matter where they live, they have the right to choose where to receive medical treatment across the EU and to be compensated for it. However, in order to secure the above-mentioned rights and unleash the potential of cross-border healthcare exchange, new solutions are needed to secure the storage and cross-border exchange of health data. After the revelations of Edgar Snowden, it is more probable that widely used closed-source security solutions have serious defects and intentionally planted backdoors. It is widely accepted that real information security can increasingly be based on the openness and transparency of the security solution and the secrecy of its encryption keys.

The healthcare sector benefits from using ECSF could be increasing awareness about possible threats, their capabilities on how to work with IT devices without causing possible incidents, and constantly adapting and learning from possible threats. However, due to differences between countries, implementing a unified cyber-skills framework might be incompatible with different nations, but as Nurse, Adamos & Di Franco (2021) mentions in their report about the European cybersecurity skills framework, forming a unified framework that would take into account the needs of EU and their member states is vital for going even further in Europe's digital future.

Acknowledgements

This work was supported by the ECHO project which has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement no.830943.

References

- ECHO (2021). *Project summary*, [online], <https://echonetwork.eu/project-summary/>
- European Commission (2021). *Exchange of electronic health records across the EU*, [online], 31st August 2021, <https://digital-strategy.ec.europa.eu/en/policies/electronic-health-records>
- Global Wellness Institute (2021). *Wellness Tourism*, [online], <https://globalwellnessinstitute.org/what-is-wellness/what-is-wellness-tourism/>
- Hübner, U., Thye, J., Shaw, T., Elias, B., Egbert, N., Saranto, K., Babitsch, B., Procter, P. and Ball, M. (2019). 'Towards the TIGER International Framework for Recommendations of Core Competencies in Health Informatics 2.0: Extending the Scope and the Roles', *Studies in Health Technology and Informatics*, Volume 264: MEDINFO 2019: Health and Wellbeing e-Networks for All
- Mageit, S. (2021). 'Skills gap in healthcare IT industry causes security threats, according to new report', *Healthcare IT News*, 16th September 2021. <https://www.healthcareitnews.com/news/emea/skills-gap-healthcare-it-industry-cause-security-threats-according-new-report>
- National Institute of Standards and Technology (2021). *Workforce Framework for Cybersecurity (NICE Framework)*, [online], NIST Special Publication 800-181. https://www.nist.gov/system/files/documents/2021/05/05/NICE%20Framework%20%28NIST%20SP%20800-181%29_one-pager_508Compliant.pdf
- Nurse, J., Adamos, K. and Di Franco, F. (2021). *Addressing the EU Cybersecurity Skills Shortage and Gap Through Higher Education*, European Union Agency for Cybersecurity (ENISA). DOI: 10.2824/033355
- Romanova, G., Vetitnev, A. and Dimanche, F. (2015). 'Health and Wellness Tourism', In F. Dimanche and L. Andrades (Eds.) *Tourism in Russia: A Management Handbook*, Emerald, pp.231-287
- Tagarev, T., Pappalardo, M. and Stoianov, N. (2020). 'A Logical Model for Multi-Sector Cyber Risk Management', *Information & Security: An International Journal* 47, no. 1, pp. 13-26. <https://doi.org/10.11610/isij.4701>
- Varbanov, P. (2021). *D2.6 ECHO Cyberskills Framework*, [online], https://echonetwork.eu/wp-content/uploads/2021/03/ECHO_D2.6_Cyberskills-Framework.pdf