How to Utilize E-EWS as a Tool in Healthcare

Janne Lahdenperä, Joonas Muhonen and Jyri Rajamäki
Laurea University of Applied Sciences, Espoo, Finland
janne.lahdenpera@student.laurea.fi
joonas.muhonen@student.laurea.fi
jyri.rajamaki@laurea.fi

Abstract: ECHO (the European network of Cybersecurity centres and competence Hub for innovation and Operations) is one of the four pilot projects under the European Commission's H2020 Program. This work-in-progress paper relates to the project's task "ECHO Early-Warning Systems (E-EWS) / ECHO Federated Cyber Range (E-FCR) Demonstration Workshops" that will be implemented during 2021 and 2022. As the healthcare industry becomes more connected to the Internet, the possibilities for disastrous cyber-attacks rise accordingly. Well-performing warning systems and robust information sharing between different parties are essential tools to help prevent these attacks. The aim of this paper is to find out how to utilize E-EWS as a tool in the healthcare sector. We started by mapping out the existing Early Warning Systems related to healthcare. At the same time, we researched the different implementations of E-EWS into already existing national systems and how possible information sharing could be done. As a result, we found that there does not seem to be any widely used international Early Warning Systems in use in the healthcare field and can conclude that implementing E-EWS could have significant benefits for the whole industry. A working Early Warning System can help to prevent cyber threats and save lives. However, there are many challenges involved in the implementation. First, the healthcare field is very fragmented with many different private and national actors, and second, the structural differences between different EU countries bring their own problems. Thus, the successful implementation of E-EWS in healthcare depends mainly on how all the different actors can cooperate.

Keywords: healthcare, ECHO project, early warning, cybersecurity, information sharing

1. Introduction

Several countries classify healthcare as one of the most critical infrastructures (Pappalardo et al., 2020). In the event of damage, the consequences will be reflected throughout the community. Digital infrastructure is part of modern healthcare and new technologies are also being used in various sectors of healthcare. This increases the number of threats related to information and cyber security. The most serious cyber threats in the near future can be considered to be cyber-attacks on healthcare (O'Brien et al., 2020).

To develop a common cybersecurity strategy for Europe, the European Commission has, under the H2020 Program, formed the European network of Cybersecurity centres and competence Hub for innovation and Operations (ECHO) project. One of the aims of the ECHO is to strengthen the cyber defence of the European Union by supporting secure collaboration between EU members.

Healthcare is made up of many different actors, including hospital environments, the pharmaceutical industry and various healthcare facilities. One of ECHO's objectives is to protect these interests. The ECHO Early Warning System (E-EWS) can be used to improve the defence against cyber threats to the healthcare system throughout the European Union. A well-designed E-EWS enables real-time data sharing between different countries and actors, thus improving the ability to defend against various cyber threats. ECHO's Federated Cyber Range (E-FCR) supports the shortage of health threats and can be used to learn how to use the E-EWS environment and to create different scenarios (ECHO, 2021).

The main goal of this work-in-progress paper is to find out how to utilize the ECHO Early Warning System as a tool in healthcare. After the introduction, section 2 familiarizes us with the different cyber threats the healthcare industry faces, and section 3 deals with early warning systems in operational use. Section 4 proposes how E-EWS can be implemented in the healthcare sector. Finally, section 5 concludes the paper and suggests future actions.

2. Cyber threats in healthcare

Healthcare faces a wide range of cyber threats, and it is highly vulnerable to these factors. According to the European Union Agency for Network and Information Security (ENISA), the most important cybersecurity challenges of healthcare infrastructures and systems are: 1) systems availability; 2) lack of interoperability; 3) access control and authentication; 4) data integrity; 5) network security; 6) security expertise and awareness; 7) data loss; 8) standardization, compliance, and trust; 9) cross-border incidents; and 10) incidents management

(Liveri, Sarri & Skouloudi, 2015). The number of cyber-attacks has increased significantly in recent years. This has been driven by the COVID-19 pandemic and the increased use of technology in the pharmaceutical industry and patient care. The operating environment for healthcare is diverse and includes many systems, data and equipment that are critical to operations. The impact of cyber-attacks on health care can be very harmful and, at worst, totally devastating. They have a direct impact on patient safety and thus on human lives. In a survey conducted by O'Brien et al (2020), none of the reported impacts of serious cyberattacks (N=9) include direct loss of life (Table 1), but as the number of attacks increases, so does the likelihood of fatalities.

Table 1: Reported impact of the most serious cyber attack

Impact	Amount
No effect	44%
Patient appointment cancelled	11%
Impact on internal project progress	11%
Opportunity costs (remediation work)	11%
Work systems down	11%
Data lost	11%

According to O'Brien et al (2020), the most common cyber-attacks on the healthcare system have been ransomware, denial-of-service attacks, data breaches and different phishing methods. Different pandemics will most likely increase the likelihood of these threats.

The effects of cyber threats can be mitigated by security training of active health care personnel using ECHO Cybersecurity Skills Framework (E-CSF). Effective and versatile training has a big effect in reducing human error. Phishing scams are less likely to be successful, as trained personnel are able to handle information, programs, and networks with caution (Pappalardo et al., 2020). However, this does not prevent the attacks from taking place.

Cyber-attacks on healthcare are mostly driven by financial goals. However, these goals may change in the future to other goals that appropriately seek to compromise patient safety. Such threats are caused by cyber warfare as well as terrorism, which have different motivations. The damage they cause to healthcare can be immeasurable. From the point of view of the cyberwar, healthcare is a strategically interesting target, as its effects extend to the army as well as to civilians (Wairimu, 2021).

3. Existing early warning systems

One example of operational early warning systems is Havaro, with Havaro 2.0 under development. Havaro operates in Finland under the auspices of the national cyber security centre Traficom (Rajamäki et al., 2019). Simola and Lehto (2020) have studied Havaro as a part of the E-EWS. It can be assumed that similar early warning systems are also in use in several European Union countries. Unfortunately, there is very little literature on the use of early warning systems in healthcare related to cybersecurity. This may be because these are individual players whose customers are in the private sector.

For non-EU actors such as the UK Cyber Security Centre (NCSC), the Early Warning System is provided in its own domain (National Cyber Security Centre, 2021). This is a similar concept to Havaro. Regarding North Atlantic Treaty Organization (NATO) member states, Dupuy et al (2020) stress the importance of creating operating models that provide early warning systems for attacks against NATO's energy sector, but there is no information if these systems have been built and if they could also be used in the healthcare sector.

4. E-EWS implementation proposal for the healthcare sector

At its core, E-EWS is an information-sharing platform. Communication between different organizations is based on mutual trust (Kirkov et al., 2020). If this trust is abused and false data entered into the system, the results can be disastrous. As the healthcare industry field is very fractured into multiple national and private actors, adding new organizations to E-EWS is not simple. One way to implement this would be to have primarily national warning systems implementing E-EWS and have different private and national health care providers get their information from these national systems.

There has already been some research into how the Finnish EWS Havaro could share information with E-EWS (Rajamäki, 2019). There would be one centralised hub for the system and many national sub-hubs. The participants do not exchange information directly with each other, because all of the information exchange is done between hubs. In this way, all of the participants can get their information from a trusted source.

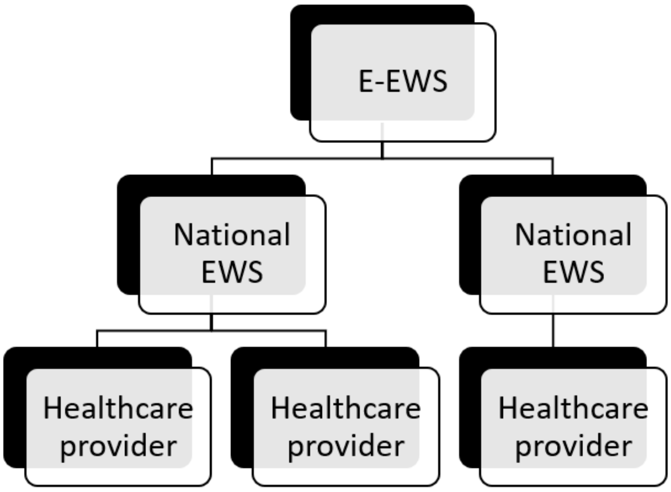

Figure 1: Proposed implementation hierarchy of E-EWS in the healthcare sector

With healthcare, this would mean that any provider that wants to be a part of the E-EWS would get their security information primarily from their national system and would not interact directly with E-EWS (Figure 1). This can also provide elasticity to the system as a whole, as it is much easier to add or remove organizations from the system. As the European Union consists of many diverse participants with their own laws and regulations, this implementation gives room for various practical ways of execution.

5. Conclusions

This work-in-progress paper starts with two questions in mind: 1) What early warning systems are there already in use in the healthcare field? 2) How could E-EWS be implemented into healthcare?

The lack of information about existing early warning systems was very surprising. It may be that the operators of these systems do not want to publicly share information about their inner workings in fear of potential security breaches. One more thing to note is that as many of the cyber threats in the healthcare industry can be best mitigated by increased training of medical personnel, the importance of EWSs may not be very high. But as the amount of networked health care equipment increases, so does the need for efficient EWSs.

The implementation of E-EWS into healthcare systems may be best carried out via national systems. The industry is very diverse and adding both national and private organizations from many different areas might prove to be very slow, difficult, and costly. By having health care providers connect primarily to their own national warning systems and only through them to the E-EWS, the operation of an EU-spanning warning system could be very manageable.

The practical implementations of E-EWS are an area that can benefit very much from further research. As the system is still primarily in the development phase, having clear and ready-made implementations could help adapt the technology for use in the healthcare field.

References

Dupuy, A., Iftimie, I., Nussbaum, D. and Pickl, S. 2020. Cyber as a Hybrid Threat to NATO's Operational Energy Security. Proceedings of the 19th European Conference on Cyber Warfare and Security (ECCWS20), University of Chester, UK, pp. 98-106.

ECHO, 2021. ECHO Federated Cyber Range, [online], https://echonetwork.eu/echo-federated-cyber-range/

Liveri, D., Sarri, A. and Skouloudi, C. 2015. Security and Resilience in eHealth: Security Challenges and Risks, ENISA.

National Cyber Security Centre, 2021. Early Warning, [online], NCSC.GOV.UK, https://www.ncsc.gov.uk/information/early-warning-service

O'Brien, N., Graß, E., Martin, G. Durkin, M. Darzi, A and Ghafur, S. 2020. Safeguarding our healthcare systems: A global framework for cybersecurity. World Innovation Summit for Health, Doha, Qatar.

Pappalardo, M. et al. 2020. D2.2 ECHO Multi-Sector Assessment Framework, [online], ECHO Network, https://echonetwork.eu/wp-content/uploads/2020/11/ECHO_D2.2-Derivation-of-ECHO-Multi-sector-Assessment-Framework_v2.4.pdf

Rajamäki, J. et al. 2019. D3.6 ECHO Information Sharing Models, [online], ECHO Network, https://echonetwork.eu/wp-content/uploads/2020/02/ECHO_D3.6-ECHO-Information-Sharing-Models-v1.0.pdf

Kirkov, P. et al. 2020. D4.3 Inter-Sector Cybersecurity Technology Roadmap, [online], ECHO Network, https://echonetwork.eu/wp-content/uploads/2020/11/ECHO_D4.3-INTER-SECTOR-CYBERSECURITY-TECHNOLOGY-ROADMAP-v1.0.pdf

Simola, J., & Lehto, M. (2020). National cyber threat prevention mechanism as a part of the E-EWS. Proceedings of the 15th International Conference on Cyber Warfare and Security (ICCWS 2020). Academic Conferences International, pp. 539-548.

Wairimu, S. 2021, e-Health as a Target in Cyberwar: Expecting the Worst. Proceedings of the 20th European Conference on Cyber Warfare and Security (ECCWS21), University of Chester, UK, pp. 549-557.