Information & Security

Published since 1998

C. Almén, N. Hagström & J. Rajamäki
vol. 53, no. 1 (2022): 11-20
https://doi.org/10.11610/isij.5301

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

ECHO Early Warning System as a Preventive Tool against Cybercrime in the Energy Sector

***Casper Almén*, *Nicholas Hagström*, and *Jyri Rajamäki* (✉)**

Laurea Leppävaara, Laurea University of Applied Sciences, Espoo, Finland
https://www.laurea.fi

ABSTRACT:

The purpose of this case study is to bring lessons learned from the ECHO project to the DYNAMO project in the energy sector. The main research question is how to understand the ECHO Early Warning System as a tool for the prevention of cybercrime as well as cyber incident coordination and response in the context of the energy sector. The applied sources of evidence are the DYNAMO project proposal, public ECHO deliverables, scientific publications available via the ECHO web pages, and other materials available via the ECHO web pages. The study shows that ECHO Early Warning System can be a very valuable tool, and it also finds examples of how to utilize E-EWS in practice. The main conclusion is that situation awareness, together with Early Warning Systems, is a powerful combination that can facilitate the fight against cybercrime.

ARTICLE INFO:

RECEIVED: 19 MAY 2022
REVISED: 18 AUG 2022
ONLINE: 19 SEP 2022

KEYWORDS:

Early warning system, ECHO project, cybersecurity, cybercrime, energy sector

Introduction

Since pretty much everything in today's world is connected to the Internet in some way or another, there need to be different methods of making it as safe as possible. Cyber security is one of the biggest parts of safely being connected to the Internet. The latest 'Threat Landscape'[1] report from the European Union Agency for Cybersecurity (ENISA) highlights major cybersecurity vulnerabilities

✉ Corresponding Author: Tel.: + 358 40 7642750; E-mail: jyri.rajamaki@laurea.fi

rooted in changes caused by the COVID-19 pandemic. The report also warns that as cyberattacks grow more advanced, existing cybersecurity measures are becoming relatively weak. One of the problems of cyber security is the overall lack of knowledge of it. In order to provide a continuous supply of services and recover fast from cyberattacks, businesses need to take into account the effects of emerging threats on their sector and their business-specific needs. The lack of knowledge is a huge issue that needs to be looked into. Thankfully there are systems available and new ones are built that try to fix this issue.

Laurea University of Applied Sciences belongs to the DYNAMO (Dynamic Resilience Assessment Method including combined Business Continuity Management and Cyber Threat Intelligence solution for Critical Sectors) consortium awarded a €5 million Horizon Europe grant to develop a new decision support platform for critical infrastructure, which will combine business continuity management and cyber threat intelligence in order to improve resilience. Led by Fraunhofer EMI, DYNAMO will combine cyber threat intelligence with business continuity management to provide a unified decision support platform. DYNAMO will build on previous H2020 solutions to provide a comprehensive platform based on end-user needs. The H2020 ECHO (the European network of Cybersecurity centres and competence Hub for innovation and Operations) project will provide a foundation for DYNAMO. The ECHO project is a huge collaboration project between European countries, the purpose of which is to boost the cyber defence of the European Union.[2] ECHO Early Warning System (E-EWS) is a near-real-time cybersecurity information sharing platform developed by the ECHO project.[3] The main purpose of E-EWS is to strengthen cybersecurity defence in European Union by sharing information between different parties and organisations.[4] The ECHO project has defined that one of the most important requirements is that connections between clients and E-EWS are secure and only authorized persons are able to access the data. Secure connections are necessary to meet the requirements of the GDPR.[4]

During the DYNAMO project, the ECHO Early Warning System will be extended in order to provide management-level decision support and the ECHO Federated Cyber-Range (E-FCR) network will provide access to cybersecurity training and emulations. One of DYNAMO's pilot cases will be the energy field. E-EWS stated by the ECHO project is a technology whose objective is to strengthen the cyber security defence. E-EWS does this by effective and efficient collaborative information sharing.

Laurea University of Applied Sciences' pedagogical model has been learning by developing (LbD), which has operated for about 20 years and is based on authenticity, experiential learning, partnership, creativity, and research.[5] Based on LbD, Laurea has developed a multiple-case study research-based approach that can integrate the university's teaching function to serve both basic and applied research, while the quality of education continues to improve.[6] This individual case study is part of the multi-case study carried out in the spring of 2022, which purpose is to bring lessons learned from the ECHO project to the DYNAMO project.

We chose the ECHO Early Warning System as the case for our case study because we see the importance of a system like that. We want to see these kinds of systems integrated more into every company. We focused this case study on the field of energy. We chose this field because there are certain issues related to cyber security such as lack of authentication, lack of knowledge, and digitalization of the field. We combined information from different ECHO publications and other material provided via the ECHO project's web pages. Our main goal is to raise awareness of the importance of working together to gain a common goal.

Our main research question for this research was "How to understand the ECHO Early Warning System as a tool for prevention of cybercrime as well as cyber incident coordination and response in the context of the energy sector". Sub-questions were:

- What are the main cyber security threats in the energy sector?
- Why is E-EWS important to the energy sector?
- How to use E-EWS in energy environments?
- How to take full advantage of E-EWS with E-FCR?
- What other early warning services are available?
- How to raise cyber awareness in the energy sector?

The outline of this paper is that after this introduction, section 'methods' provides a detailed description of the methods and procedures used in the study. Then, section 'results' answers to the research sub-questions. And finally, section 'conclusions' tries to answer the main research question and concludes the paper.

Methods

According to Yin[7] (2009), a case study analysis relies on multiple sources of evidence with data needing to converge in a triangulation fashion, and it benefits from the prior development of theoretical propositions to guide data collection and analysis. Here, the term "triangulation"[8, 9, 7] refers to the usage of multiple sources of evidence such as (1) data sources as data triangulation; (2) among different evaluators as investigator triangulation; (3) perspectives of the same data set as theory triangulation, and (4) an approach as methodological triangulation. This research has mainly used data triangulation and utilized data sources that are:

- DYNAMO project proposal[10]
- public ECHO deliverables[11]
- scientific publications available via the ECHO web pages[12]
- other materials available via the ECHO web pages, such as blogs, presentations, and videos.

Our methods for this case study were qualitative content analysis. We conducted a literature review and read various documents to be able to answer the research question. We gathered as much data as possible to get a good overview of the subject. We gathered data that can be analysed and combined into a single case study. After this, we combined this information and gave a few examples of how the ECHO Early Warning System can be beneficial to the energy sector.

Results

Cyber security threats in the energy sector

The energy sector is a big part of everyone's daily life directly and indirectly. Energy is the source of almost everything. Without access to energy, our society would not function at all. Our banks, houses, stores, and even cars would simply not be usable if the energy sector did not function as intended. Even our running water is connected to the energy sector and probably would not function. These kinds of lack of access to human's basic needs would create chaos in our society. The energy sector, as the name implies, is the sector that is responsible for supplying our energy. Examples of parts of the energy sector are electric, coal, gas, and oil companies. The main part of the energy sector is to provide us with electricity and heating. The energy sector is divided into two different categories, which are non-renewable- and renewable energy. There are thousands of companies around the world that work in both categories of the energy sector. The energy sector, as every other sector, has its flaws and issues that need to be addressed. The flaws and issues can be used to do a cyber-attack against the companies in the field of energy. Attacks on this sector can lead to catastrophic outcomes. Attacks on the energy sector can lead to problems like loss of power, service interruptions, and even natural disasters.

According to ECHO D2.1[13] in the energy sector, there are many systems and tools that are used all the time. These are called programmable computing systems. Usually, these are automation systems that are used to provide the functionality of the facilities in the energy sector. These systems are rarely restricted and are accessible to anyone inside the perimeters. These systems can also usually be remotely configured, which implies that proper measurements should take place to limit the remote access as safely as possible. The problem with these systems in the energy sector is that the systems rarely have any kind of authentication. This means that almost anyone who knows how to get into these systems can do it. By analysing the provided problems, these systems need to be secured and restricted access. There are known attacks in the energy sector. The most known ones are Stuxnet virus, Black energy malware, and Industroyer malware. These attacks need to be analysed.

The specific threats to the energy sector, listed by ECHO D2.1, are:

- Smart meters are used to gain access into the power system
- Power system can be used to gain access into civil infrastructure
- Disruption of the systems

- Electricity market attacks
- Large area blackouts
- Tampering with electricity consumption usage
- Modifying the schedule of the power-generating unit.

Why is E-EWS important to the energy sector?

Industrial Control Systems (ICS) are command and control networks and systems designed to support industrial processes. The largest subgroup of ICS is SCADA (Supervisory Control and Data Acquisition) systems. Nowadays, ICS and SCADA systems are widely used in many sectors, including the energy sector. These kinds of systems help organisations with process control, automation, and safety. In the future, the role of automation will keep increasing, and the role of ICS and SCADA systems will be emphasized. Connecting control systems to networks and IT environments will highly increase the attack surface and expose critical infrastructure to cyber-attacks.[14] One monitoring tool that should be used in critical environments is utilizing logs. There are a lot of different ways to manage logs. One good example is a SIEM (Security Information and event management) system. SIEMs provide a centralized place to store logs from multiple systems and make log management a lot easier. We think that every party managing critical infrastructure should have a SIEM-like system in use.[15] The energy sector in the world has faced direct cyberattacks in recent history. Two famous cases are the 2010 Stuxnet and the 2015 cyberattack on the Ukrainian power grid. Another good example is the ongoing cyberwar between Israel and Iran. This war has escalated in 2020 and 2021 into targeting civilian infrastructures. These cases show how vital cybersecurity itself is to the energy sector, how an early warning system could be beneficial and why it is important. E-EWS aims to provide smooth information exchange that is combined in one place and available for authorized partners.

How to use E-EWS in energy environments?

ECHO early warning system (E-EWS) is a tool that is used to improve and strengthen proactive cyber defence by effective and efficient information sharing. The tool is used to gain trusted cooperation among multiple parties in the scene of cyber security. It offers great trustworthy incidents handling and collaboration capabilities. These can be used in the early stages of attacks and in the rest of the attack timeline. The goal of the tool is to support and enhance the computer/cyber incident response teams, or CIRTs), and security operation centres (SOCs) activities. E-EWS uses warnings as its main trait. These warnings are then shared between the partners. These warnings are then analysed and used to build a rich data model. This is a model that is usable via humans or machines. The warnings provide a big set of attributes to records that can be used.

E-EWS is based on tickets that are made for example from security incidents. When a security incident happens, the organisation should create a ticket to ECHO early warning system. The ticket consists of basic information like title, description, and participants. There is also a possibility to attach external files. This is where the log management system comes in. If an organisation has a log management system in place, they could just attach a copy of logs from the time of the security incident. Log files are greatly valuable to other organisations because of all the details they include for example Tactics, Techniques, and procedures (TTPs). By sharing logs between organisations, it is possible to achieve better cyber defence between the energy industry and European Union. E-EWS also gives Organisation's possibility to find near-real-time threats from the early warning system database. The database includes information about cyber threats that other organisations have noticed. For example, if you are an energy company in Belgium, it is possible to get threat information from an energy company in France. Another valuable benefit of the ECHO early warning system is notifications. It's possible to get alerts in near-real-time from an early warning system about security incidents that the organisation is interested in. As Figure 1 presents, based on alerts, it is possible to make further actions in real-time.

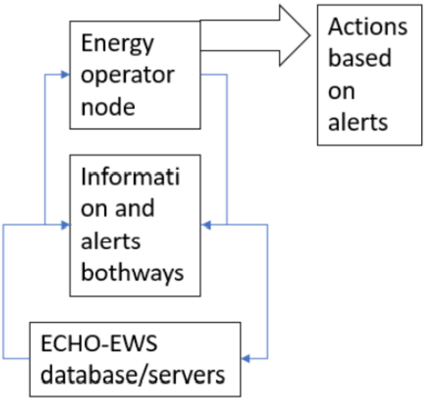

Figure 1: E-EWS use in the energy sector.

Taking full advantage of E-EWS with E-FCR

ECHO Early Warning System collects data from various nodes of the federation and constitutes the main source of trends and threat intelligence data. For example, in our case, we study top threats to the energy sector. With the information collected, EWS can provide inputs to the cyber range and content providers while designing new cyber range services to be published in the ECHO federated cyber range. By connecting the core system of the ECHO Federated Cyber Range to the ECHO Early warning system, providers could retrieve valuable information for their content development activities based on real-world needs. [4 p. 75.] Regarding the explanation of early warning systems collecting data and forming top threats for the energy sector and providing this information to the federated cyber range content providers, the energy sector could get realistic cyber ranges to raise their cyber awareness against threats.

Other early warning services

We found out that there are some similar early warning systems and services to E-EWS. One example of a similar service is Havaro, the national information sharing system developed by the Finnish Cybersecurity Centre (Kyberturvallisuuskeskus). Havaro is very similar to ECHO Early Warning System with the exception that Havaro is only a national service, whereas EEWS is a service shared between European Union.[16]

Raising Cyber-awareness

As we stated before, the energy sector has a lot of technical issues that can be breached and exploited. But there is also the human element that is critical to remember and understand.

Our next research sub-question for this case study was *how to raise awareness about cyber threats in the energy sector*. This basically means how companies and organisations can maximize their knowledge about cybersecurity threats and attacks.

In ECHO D2.1, there are numerous case studies where the lack of understanding is one of the causes of security incidents happening in organisations and in the energy sector as a whole. In descriptions of different scenarios, it is explained that social engineering and the lack of awareness can lead to serious consequences that could put entire systems in jeopardy. Some organisations have security policies that are either obsolete or not implemented correctly, which could lead to these security incidents if something is not done to this issue.

In ECHO D3.6 [17] and the DYNAMO project proposal, the authors mention one key term where information sharing revolves: “situation awareness.” This is an important element that could solve the critical problem of security incidents. It basically means how a person can understand the current situation (in this context, a security incident) and how their actions will impact the situation. If the person knows what they are doing, they can identify, protect, and prevent possible threats that are jeopardizing the targeted systems. Also, if the incoming attack is successful, this person knows how to recover from it as efficiently as possible. This level of understanding and awareness can be achieved by having a proper security policy in an organisation which includes good training for all employees and constant development on the cybersecurity field.

Considering Early Warning Systems, they are able to help the users tremendously when dealing with possible threats and attacks. But it is important to note that even these systems can be rendered useless if the users behind them are not certain what to do in difficult situations. Especially when it is sharing information between different departments or even just individuals, situation awareness is a very important ability to have. Also, if the Early Warning Systems themselves give false positives or negatives, situation awareness helps a lot when analysing the warnings and alerts.

Conclusions

This case study researches how we can understand the ECHO Early Warning System as a tool for the prevention of cybercrime as well as cyber incident coordination and response in the context of the energy sector. In answer to this question, we first defined the energy sector and what kind of issues and threats it can have in the cybersecurity field. We stated that it is very important that this sector is secured from cyber threats because of its importance to society. One of the best tools for fighting cyber threats is the Early Warning System, which increases cyber defence by effective information sharing. Even though the EWS name states that it is used especially in the early stages of a possible attack, they are still useful throughout the whole process.

We further found out that industrial control systems and SCADA systems are vulnerable and can be exploited by cybercriminals and state actors. There have been many recent cases of these exploitations that prove how important cybersecurity is for the energy sector. As we analysed the DYNAMO project proposal, public ECHO deliverables, scientific publications available via the ECHO web pages, and other materials available via the ECHO web pages, we concluded many of the attack scenarios could have been prevented if an EWS was in use. Our main result to our research question is that ECHO Early Warning System can provide valuable resources to the energy sector so that energy companies can secure the availability and performance of their infrastructure in the event of a cyber threat, and E-EWS can be a very valuable tool to prevent these kinds of attacks

One of our research sub-questions was about how to raise cyber awareness in the energy sector. We concluded that all of the people in a certain company or organisation should have some kind of understanding of cybersecurity-related subject matters and issues. This means that not only should the company's main leadership know about it but also the regular employees as well. As we stated before, not all companies and organisations are focusing sufficiently on this issue which can be one of the biggest security weaknesses in their day-to-day business. If the overall awareness level is high, security breaches and incidents are decreased tremendously since, in these situations, everyone should have at least some kind of knowledge on how to react and what to do. One of the best solutions to this problem is to have sufficient training programs in the organisations that teach every employee the needed knowledge so the information sharing and overall communications work in harmony. Situation awareness together with Early Warning Systems is a powerful combination to fight against cybercrime.

This paper brings lessons learned from the ECHO project in the energy sector to the DYNAMO Horizon Europe project that will provide an essential tool for the business continuity of critical infrastructure organisations. The tool considers the latest situation about cyber threats and will deliver decision support across all stages of the resilience cycle (prepare, prevent, protect, respond, and recover) on a single platform that is tailored to the needs of critical infrastructure. That will have wider benefits for other organisations and for societal security.

Acknowledgement

This work is done as a final assignment during the Cybersecurity Project Course at Laurea University of Applied Sciences in spring 2022. We would like to thank Sakari Kuosmanen, Johannes Taskinen, and Eemil Kangas-Korhonen, the students of previous implementations of the course, for the background material they produced for this article.

References

[1] "ENISA Threat Landscape (ETL) Report – 2021," ENISA, October 2021, https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends.

[2] ECHO, "Project summary," 2022, https://echonetwork.eu/project-summary/.

[3] Fabrizio De Vecchis, "Technology which aims to strengthen the proactive cybersecurity defense of the European Union," ECHO Early Warning System (E-EWS), 2022, https://echonetwork.eu/echo-early-warning-system-e-ews/.

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

[5] Rauno Pirinen and Maarit Fränti, "Learning by Developing," in *Information Technologies: Theory, Practice, Innovations, International Conference, Alytus College*, 2007.

[6] Jyri Rajamäki and Rauno Pirinen, "Resilient Learning as a Tool for Excellence: Laurea's Students in the ECHO H2020 Project during the COVID-19 Pandemic," *2022 IEEE Global Engineering Education Conference (EDUCON),* 2022, pp. 1889-1894, https://doi.org/10.1109/EDUCON52537.2022.9766796.

[7] Robert K. Yin, *Case Study Research Design and Methods,* 4th ed. (Thousand Oaks, CA: Sage Publications, 2009).

[8] Michael Patton, *Qualitative Evaluation and Research Methods*, 2nd ed. (London: Sage Publications, 1990).

[9] Robert Winter, "Interview with Jay F. Nunamaker, Jr. on "Toward a broader vision of IS research," *Business and Information Systems Engineering* 5 (2010): 321–323.

[10] "Dynamic Business Continuity and Recovery Methodologies Based on Models and Prediction for Multi-level Cybersecurity," DYNAMO Prosal ID 101069601, Topic HORIZON-CL3-2021-CS-01-01, 2021.

[11] ECHO Deliverables – ECHO Network, 2022, https://echonetwork.eu/deliverables/.

[12] ECHO Publications – ECHO Network, 2022, https://echonetwork.eu/publications/.

[13] Nikolai Stoianov and Maya Bozhilova, "ECHO D2.1. Sector Scenarios and Use Case Analysis" (2019).

[14] Rossella Mattioli and Konstantinos Moulinos, "Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors," ENISA, 2015, https://www.enisa.europa.eu/publications/maturitylevels/at_download/fullReport.

[15] Gianfranco Cerullo, Valerio Formicola, Pietro Iamiglio, and Luigi Sgaglione, "Critical Infrastructure Protection: having SIEM technology cope with network heterogeneity," 2014, *arXiv preprint arXiv:1404.7563*, https://arxiv.org/abs/1404.7563.

[16] National Cyber Security Centre, "Havaro service," 2022, https://www.kyberturvallisuuskeskus.fi/en/havaro-service.

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

About the Authors

Casper Almén and **Nicholas Hagström** are third-year students at Laurea University of Applied Sciences in the Business Information Technology (BIT) Programme. They both have focused their studies on information security and cybersecurity courses.

Jyri Rajamäki is Principal Lecturer in Information Technology at Laurea University of Applied Sciences and Adjunct Professor of Critical Infrastructure Protection and Cyber Security at the University of Jyväskylä, Finland. He holds D.Sc. degrees in electrical and communications engineering from Helsinki University of Technology, and a PhD in mathematical information technology from University of Jyväskylä. He is the Responsible Teacher of the cybersecurity project course and supervisor of the student's project work.