https://doi.org/10.52326/ic-ecco.2021/NWC.02

Implementing Design Science Research Method to Develop a Cyber Security Framework for HEIs in Moldova

Alexei Arina
Technical University of Moldova, 168, Stefan cel Mare Bd., MD-2004, Chisinau, Republic of Moldova
arina.alexei@tse.utm.md

***Abstract*— This scientific paper presents how a problem in the field of cybersecurity can be solved by using the scientific method Design Science Research (DSR). The research problem is the lack of a comprehensive cyber security framework that meets international security standards for HEIs (Higher Education Institutions) in Moldova. Although the need for a centralized approach to cybersecurity in university networks, which are decentralized and open by design, is increasingly emerging with the digitalization of HEI. Thus, actions were identified for each stage of the DSR method, which as a result will produce a cyber security conceptual framework (CSCF) for increasing cyber security in HEIs.**

Keywords*— *DSR method; framework; cyber security; HEIs; ISO27001.

I. Introduction

Universities currently provide several services based on communication networks. Thus, HEIs (Higher Education Institutions) have become dependent on Information and Communication Technologies (ICTs), in order to provide digital educational and research services, indispensable in the 21st century.

Unfortunately, recent researches have highlighted an impressive increase in cyber-attacks within HEIs in 2020 [1]–[4], which makes the situation alarming and requires prompt reactions. Insufficient knowledge of the risks associated with information assets can significantly damage the activity of HEIs [5]. It is necessary to consider support assets such as: network devices, applications, human resources, infrastructure; that are used to protect the primary assets of HEIs such as:

-business processes: online courses, exams, IT infrastructure for students or dedicated applications;

-information: research data and personal data, intellectual property or dissertation materials, financial records.

Thus, cyber security will play an increasingly important role in the activity of HEIs, in the next period. Cyber security has been defined by the International Communications Union (ITU) to mean "a 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 organization and user's assets" [3]. Researchers recommend the implementation of cybersecurity frameworks, to achieve proper protection in the campus network [6], [7].

The framework can be defined as a network or a plan of interconnected concepts, which provides a comprehensive understanding of a phenomenon [7]. Approaching cybersecurity in HEIs by implementing a conceptual framework will allow the combination of several existing concepts so that the framework created is one focused on the activity of HEIs and effectively protects cyber security.

In this scientific article, the method of Design Science Research (DSR) proposed by the author to develop a cyber security conceptual framework (CSCF) for HEIs in Moldova was analyzed. Without a strong component that produces explicitly applicable research solutions, research in the cyber security field, faces the potential of losing influence over research streams for which such applicability is an important value [9]. The actions and what were achieved for each stage of the DSR method were established, in order to understand how the CSCF was developed and the result of the scientific study to be reproducible.

Thus, the second section of this work will describe the research problem, in the third section the reasons for selecting the DSR method were established, the fourth section will describe the process by which DSR contributed to the development of CSCF for HEIs in the Republic of Moldova. The last section is reserved for conclusions.

https://doi.org/10.52326/ic-ecco.2021/NWC.02

II. BACKGROUND

The need for comprehensive research, to create the CSCF for Higher Education Institutions in the Republic of Moldova, was based on:

- the survey in which the stakeholders of the Information Technology departments from the 9 largest state institutions in the Republic of Moldova participated. The results of the survey show that HEIs are not certified with any standards for information security and do not have an authorized cybersecurity framework;
- the literature review of research articles about how to ensure cyber security in HEIs, which elucidated the problem of insufficient research regarding the cyber security frameworks implemented in the HEI.

Researchers have differing views on the cybersecurity framework that would be appropriate for HEIs, however the following standards prevail: ISO27001, COBIT and ITIL. The problem is that standards are oriented of commercial organizations, that why is difficult to implement them in universities [10]–[12].

The research problem can therefore be defined as:" the lack of a cyber security framework for HEIs in the Republic of Moldova". The development of CSCF would solve this problem.

In the field of cyber security, in Moldova, exists the Government Decision 201 (GD.201), of 28-03-2017, on the approval of the Mandatory Minimum Cyber Security Requirements [13], that refers to all public organizations, without a special emphasis on the specifics of HEIs, moreover, in a paper previously published by the author [14], multiple gaps were identified between DG201 and ISO27001.

III. DESIGN SCIENCE RESEARCH METHOD

The challenge was to select a method that would allow the creation of a product, a security framework that would solve cybersecurity issues in HEIs. This premise was the basis for identifying the scientific method Design Science, intensely used internationally, the finality is an artifact that can be a model, concept or framework [15]–[17].

DSR is defined as "a problem-solving paradigm that seeks to improve knowledge by creating innovative artifacts" [15]. Another approach to DSR is "research in design science (DSR), also known as constructive research, is a methodological approach concerned with the design of artifacts that serve human purposes" [18].

The result of this type of research, as already mentioned, is an artifact that solves a problem in the field, also known as the concept of solution, which must be evaluated by criteria of value or utility [18]. The DSR method has been appreciated as one of the main research methods for engineering [18].

DSR projects must offer both intellectual merit in creative design and extended impact in the application field through original solutions to the research problem [16], [17]. This is seen as an opportunity to demonstrate the rigor and relevance of Information Systems as an academic field [19], [20], and Information Systems research should help address real-world challenges [21].

Research is linked to the need for solutions to be investigated empirically with specialists from organizations using specific technology [15]. Often, the analysis of the business environment and the derivation of the specific needs to be addressed build the starting point of a DSR project. However, there are also situations where the needs have already been studied and can be taken from existing research [15].

DSR aims to create an innovative solution to the problem, which in most cases builds on the existing components of a solution and combines, revises and expands existing design knowledge [15]. Simon [22] stated that "solving a problem means presenting it so that the solution becomes transparent".

The literature identifies 6 typical stages of the DSR project: problem identification and motivation, definition of objectives for solution, design and development / design of the artifact, demonstration, evaluation, followed by communication of results [9], [15], [23]. In the next section will be assigned the specific actions for each stage of DSR, to develop CSCF artifact.

IV. COMMUNICATION OF RESULTS

In order to solve the research problem, the DSR method was used, which allowed the creation, development and evaluation of CSCF artifact, which can be later implemented to increase cyber security in HEIs, as long as this scientific method focuses on solving a specific problem in the field [15], [16]. Figure 1 shows the actions performed according to the DSR stages.

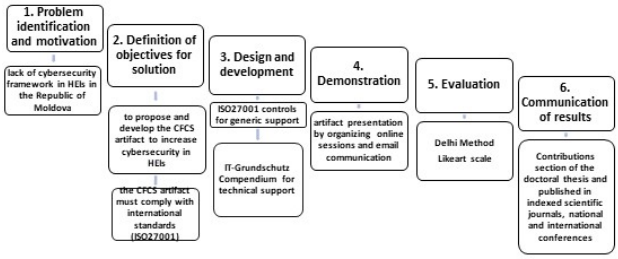

Figure 1. DSR stages

A. Problem identification and motivation

Due to decentralized networks, consisting of several small networks, opening to the Internet [18], to provide extensive educational services to students, HEIs are vulnerable to various cyber-attacks. Due to the impressive amount of personal data or research data with which it operates, it is of great interest to cyber attackers. However, HEIs in the Republic of Moldova are not certified with any security standard and have not implemented a comprehensive cyber security framework such an Information Security Management System that is

https://doi.org/10.52326/ic-ecco.2021/NWC.02

recommended by ISO27001, or another cyber security framework.

B. Definition of objectives for solution

The objective was to develop a cybersecurity conceptual framework for HEIs, based on the security standard ISO27001, to comply with the Bologna process, which defines the importance of implementing frameworks internationally recognized as an extremely important process. The challenge was to identify the value criteria for the CSCF artifact. The proposed criteria and arguments can be seen in Table 1.

Table 1. Criteria of value

Nr	Criterion	Arguments
1	Target group oriented	Contain controls corresponding business processes in academia
2	Implementation phases	The artifact must determine the main steps after which the cybersecurity framework will be implemented within the HEI
3	Predefined roles	The roles of staff involved in the implementation of cybersecurity in HEIs must be clearly defined, in order to know the responsibilities of the post and to designate the owners of critical assets.
4	Risk management	In order to increase the effectiveness of the security framework, it is necessary to identify the real risks, related to the critical assets and the threats that may affect them. To assess the impact of risks.
5	Efficient	The efficiency of the artifact depends directly on how well it is understood by HEI specialists, who are going to implement it. How clearly the objectives, purpose and implementation phases were defined.
6	Scalable	It can be implemented in any institution, regardless of its size and the complexity of the services it provides
7	International importance	The security framework for HEIs must comply with international standards in this field, and subsequent certification of institutions is an appreciable objective.

The Delphi method was used to evaluate the CSCF artifact, as it is suitable for obtaining expert recommendations when designing a new information system [24], that solves a problem in the real environment. The generic characteristics of the Delphi method are: selection of experts, creation of a panel (repetitive investigation method to follow the evolution of a phenomenon through requests for information, at pre-established intervals, from the same groups of people), anonymity of participants, iterations and feedback [24].

C. Design and development

The development of the CSCF artifact was based at the initial stage on the review of the literature to identify the security frameworks for HEIs, recommended by researchers, the security standards analyzed through their implementation in academic institutions and the current state of research in this field. Thus, it was established that the development of the CSCF artifact is based on ISO27001. But the big challenge has been to determine how ISO27001 controls can be implemented, being generic. Thus, it was established that the development of the CSCF artifact should be achieved through the synergy of ISO27001 and IT - Grundschutz Kompendium which is a technical guide containing the necessary tools for the implementation of security controls. And finally, interdependencies were created between university business processes and support assets.

D. Demonstration

After the CSCF artifact was created, it was presented to the selected experts and stakeholders. The Likert scale, often used in many scientific articles [25], [26] was subsequently proposed to evaluate the artifact in the light of the value criteria set out in point B. Thus, in order to demonstrate the effectiveness of the criterion, it was necessary to place it between 4 “Highly efficient” and 5 “Most efficient”, the criterion was assessed as suitable for the validation of the artefact.

E. Evaluation

This activity should determine how much the CSCF artifact supports solving the research problem [1], this is possible in view of the objectives set out in point B, compared to the result of point D.

The qualitative method of evaluating the artifact was used, through several Delphi rounds, which allowed obtaining the evaluation through empirical evidence (feedback from experts and specialists in the field) and evidence proven by applying the international standard ISO27001. The qualitative approach facilitates a better understanding of the perceptions, beliefs and attitudes of the participants in the philosophical interpretive study of information systems [27]. The qualitative method allows to understand the context of a solution, including based on the comments made by HEIs specialists.

Thus, for the initial evaluation, the CSCF artifact was presented to the experts for evaluation, a great value representing the recommendations given by the experts. Subsequently, for empirical evaluation, the CSCF artifact was presented to HEIs stakeholders. The post-implementation feedback will be presented after the CSCF artifact will be implemented for a certain period of time in the HEIs of the Republic of Moldova.

F. Communication of results

The communication of the results took place through the publication of scientific articles and participation with communiqués at national and international conferences.

https://doi.org/10.52326/ic-ecco.2021/NWC.02

Thus, the criteria according to which the CSCF artifact was developed, the novelty of the product and how it will have an impact on the increase of cyber security in the HEI will be exposed. The CSCF artifact was presented to both the technology-oriented and the management-oriented public. This will allow practitioners to reap the benefits of the CSCF artifact, and researchers to build a cumulative knowledge base for further extension and evaluation of the artifact [2].

V. CONCLUSIONS

The DSR method was the research method selected to develop the conceptual framework for increasing cyber security in HEIs in Moldova.

This research method is qualitative, in order to obtain qualitative results, the Delphi method was selected, and the Likert scale to evaluate the value criteria of the proposed conceptual framework.

The chosen scientific method made it possible to identify the steps needed to solve the identified research problem, so it can be concluded that it is effective in the field of cyber security.

REFERENCES

[1] Kaspersky, "Education Report," 2020. [online]. [accessed: 1.08.2021].Available: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2020/09/04113558/education_report_040 92020_2.pdf.

[2] A. Alexei and A. Alexei, "Cyber Security Threat Analysis In Higher Education Institutions As A Result Of Distance Learning," in *International journal of scientific & technology research*, vol. 10, no. 3, Mar. 2021.

[3] A. Alexei, "Network Security Threats to Higher Education Institutions," in CEE e|Dem and e|Gov Days, May 2021, pp. 323–333, doi: 10.24989/ocg.v341.24.

[4] JISC, "Cyber Impact Report," 2020. [Accessed: 5.08.2021]. [Online]. Available: https://repository.jisc.ac.uk/8165/1/cyber-impact-report.pdf.

[5] E. W. N. Bernroider, S. Margiol, and A. Taudes, "Towards a General Information Security Management Assessment Framework to Compare Cyber-Security of Critical Infrastructure Organizations," in: CONFENIS 2016. Lecture Notes in Business Information Processing, vol 268. Springer, Cham. https://doi.org/10.1007/978-3-319-49944-4_10.J.

[6] A. Itradat, S. Sultan, M. Al-Junaidi, R. Qaffaf, F. Mashal, and F. Daas, "Developing an ISO27001 Information Security Management System for an Educational Institute: Hashemite University as a Case Study," in: *Jordan Journal of Mechanical & Industrial Engineering*, vol. 8, no. 2, pp. 102–118, 2014.

[7] G. Disterer, "ISO/IEC 27000, 27001 and 27002 for Information Security Management," in: *Journal of Information Security*, vol. 04, no. 02, 2013, doi: 10.4236/jis.2013.42011.

[8] Y. Jabareen, "Building a Conceptual Framework: Philosophy, Definitions, and Procedure," in: *International Journal of Qualitative Methods*, vol. 8, no. 4, Dec. 2009, doi: 10.1177/160940690900800406.

[9] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A Design Science Research Methodology for Information Systems Research," in: *Journal of Management Information Systems*, vol. 24, no. 3, Dec. 2007, doi: 10.2753/MIS0742-1222240302.

[10] J. Merchan-Lima, F. Astudillo-Salinas, L. Tello-Oquendo, F. Sanchez, G. Lopez-Fonseca, and D. Quiroz, "Information Security Management Frameworks and Strategies in Higher Education Institutions: A Systematic Review," in: *Annals of Telecommunications*,Jul. 2020, doi: 10.1007/s12243-020-00783-2.

[11] S. E. Donaldson, S. G. Siegel, C. K. Williams, and A. Aslam, "Cybersecurity Frameworks," in: *Enterprise Cybersecurity*, Berkeley, CA: Apress, 2015.

[12] H. Rehman, A. Masood, and A. R. Cheema, "Information Security Management in Academic Institutes of Pakistan," in: *National Conference on Information Assurance*. Dec. 2013, doi: 10.1109/NCIA.2013.6725323.

[13] Decision 201/2017 of the Moldovan Government on the approval of the Mandatory Minimum Cyber Security Requirements. In: Official Monitor. 07.04.2017, L 109-118/277. [Accessed 2.08.2020].Available: https://mei.gov.md. [in Romanian].

[14] A. Alexei, "Ensuring Information Security in Public Organizations in The Republic Of Moldova through the ISO 27001 Standard," in: *Journal of Social Sciences*, vol. IV(1), Mar. 2021, doi: 10.52326/jss.utm.2021.4(1).11.

[15] vom Brocke J., Hevner A., Maedche A. "Introduction to Design Science Research," in: vom Brocke J., Hevner A., Maedche A. (eds) Design Science Research. Cases. Progress in IS. Springer, Cham. https://doi.org/10.1007/978-3-030-46781-4_1I.

[16] Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). "Design science in information systems research," in: MIS Quarterly: Management Information Systems, 28(1), 75-105. https://doi.org/10.2307/25148625.

[17] R. Baskerville, A. Baiyere, S. Gergor, A. Hevner, and M. Rossi, "Design Science Research Contributions: Finding a Balance between Artifact and Theory," in: *Journal of the Association for Information Systems*, vol. 19, no. 5, May 2018, doi: 10.17705/1jais.00495.

[18] A. Dresch, D. P. Lacerda, and J. A. V. Antunes Jr, "Design Science Research," Cham: Springer International Publishing, 2015.

[19] Watson, Boudreau, and Chen, "Information Systems and Environmentally Sustainable Development: Energy Informatics and New Directions for the IS Community," *MIS Quarterly*, vol. 34, no. 1, 2010, doi: 10.2307/20721413.

[20] A. S. Lee, M. Thomas, and R. L. Baskerville, "Going back to basics in design science: from the information technology artifact to the information systems artifact," in: *Information Systems Journal*, vol. 25, no. 1, Jan. 2015, doi: 10.1111/isj.12054.

[21] J. Becker, J. vom Brocke, M. Heddier, and S. Seidel, "In Search of Information Systems (Grand) Challenges," in: *Business & Information Systems Engineering*, vol. 57, no. 6, Dec. 2015, doi: 10.1007/s12599-015-0394-0.

[22] Herbert A. Simon, "The Sciences of the Artificial", 3rd ed. London: MIT Press, Cambridge Massachusetts, 1996.

[23] Chandra Kruse L., Seidel S., vom Brocke J. "Design Archaeology: Generating Design Knowledge from Real-World Artifact Design,". In: DESRIST 2019. Lecture Notes in Computer Science, vol 11491. 2019. Springer, Cham. https://doi.org/10.1007/978-3-030-19504-5_3.

[24] R. Skinner, R. R. Nelson, W. W. Chin, and L. Land, "The Delphi Method Research Strategy in Studies of Information Systems," in: *Communications of the Association for Information Systems*, vol. 37, 2015, doi: 10.17705/1CAIS.03702.

[25] J. Kaur and N. Mustafa, "Examining the effects of knowledge, attitude and behaviour on information security awareness: A case on SME,"in: Research and Innovation in Information Systems. Nov. 2013, doi: 10.1109/ICRIIS.2013.6716723.

[26] N. Polemi, "Maritime Supply Chain Risk Assessment (at Entity Level)," in: Port Cybersecurity, pp. 67–102, Jan. 2018, doi: 10.1016/B978-0-12-811818-4.00004-6.

[27] M. D. Myers and M. Newman, "The qualitative interview in IS research: Examining the craft," in: Information and Organization, vol. 17, no. 1, Jan. 2007, doi: 10.1016/j.infoandorg.2006.11.001.