JSEG

JOURNAL OF SMART ECONOMIC GROWTH

www.jseg.ro ISSN: 2537-141X Volume 7, Number 1, Year 2022

READY FOR THE NEXT CYBER THREAT? INDISPENSABLE ASSETS FOR DIGITAL BUSINESS ORGANISATIONS

Eliza Nichifor[*], Gabriel Brătucu[*]

[*]Transilvania University of Brașov

eliza.nichifor@unitbv.ro, gabriel.bratucu@unitbv.ro

Abstract: *By intensifying the digital activity of organisations, the cybersecurity has been placed in special lights when decision-making processes are carried out. Cyber risks are considered extremely important for digital organisations development and special recommendations are highly demanded. Aiming to research new opportunities for this context, the authors promote the circumstances of cybersecurity research field by performing qualitative research. The method used was represented by visual network analysis with Java technology, an innotive tool for analysing and interpreting the network of the knowledge field. The bibliometrics such as reference, cited reference, author and institution were used to group 5,287 relevant resources from Web of Science database and mean silhouette, modularity, or betweeness centrality metrics were interpreted to validate the quality of the network. The result present the importance of human factor in cybersecurity politics, the significant topic of cybersecurity governance and regulations, and the relevance of cybersecurity culture development for employees. The study enriches the literature by introducing the most recent connections from the pandemic year, presenting the increasing awareness of the risks involved in carrying out the activity of digital organisations.*

JEL classification: D18, M15, M53.

Key words: cybersecurity, knowledge research, visual network analysis

1. INTRODUCTION

The privacy and security in the digital environment have become a top priority and a global concern (Hassib and Shires, 2022) in the use of digital tools by organisations. As the activities of digital organizations become more and more intense and the level of digitization is on an upward trend in terms of operationalization or management activities. This is leading to growing organizational threats, with management facing major cybersecurity challenges (Al-Sanjary *et al.*, 2022) and this is the reason for existing concepts such as cyber risk management or cybersecurity decision making in the literature (Aliyu, He, *et al.*, 2020). This type of risks are considered very important challenges especially for the organisations that want to grow in a virtual, ever growing space (Jbair *et al.*, 2022). The application of the concept is widely presented in the scientific world. From banking system (Mbelli and Dwolatzky, 2016; Xu *et al.*, 2020), healthcare (Spanakis, EG; Bonomi, S; Sfakianakis, S; Santucci, G; Lenti, S; Sorella, M; Tanasache, 2020; Nifakos *et al.*, 2021; Ravidas, Pattinson and Oliver, 2021) to user behaviour, (Baltezarevic and Baltezarevic, 2021; Zwilling *et al.*, 2022), the importance of cybersecurity awareness and knowledge is highly needed.

A study of digital organisations in the UK found that 50% of them represented a strong position on cybersecurity as a necessary factor in decision-making at management level. Their representatives were very confident that the budget was allocated to protection against the most important cyber threats. Regarding this aspect, the percentage is represented by 38% of the subjects, compared to 44% (globally). Asked what cybersecurity incidents might occur, 58% of participants in the same study included attacks on cloud services, critical business services (52%), and ransomware attacks (50%) (Gladman, 2021).

Also, the literature presents the perspective of education in the field. Different models that centre the priority of identifying, analysing and learning to manage risks in this knowledge research field earn a lot of recognition (Lehto, 2015; Stevens *et al.*, 2019; Du *et al.*, 2020; Martínez, 2020; Annarelli and Palombi, 2021).

Based on the pervasive challenges of the current context and the widespread application of cybersecurity, a research question has emerged that the authors posed in relation to this topic. *"What are the issues that academia and practitioners need to understand the frontiers of cybersecurity research?"* To answer the question, the researchers started a review of the literature addressing the following critical points:

- ***What are the major areas of cybersecurity research?***
- ***What is the main topic in the field of research?***
- ***How are major topics connected through specific scientific papers?***

The concept of cybersecurity has been analysed by aiming to identify and promote challenges and opportunities for digital organizations in the context of the highly required necessity to enrich the knowledge field of cybersecurity.

In this sense, the qualitative method of visual network analysis was performed, which determined a clear and a strong network of the research field by reference and author node.

The results align the work of this paper by bringing to light the necessity of increasing the competences of the employees and the human factor, as an influential aspect of digital organisational development.

2. MATERIALS AND METHODS

The method by which the analysis of the research field was approached was based on the adapted observation technique and is represented by the creation and visualization of a network, using Java technology (Chen, 2010; Glänzel *et al.*, 2019). It is an innovative qualitative method by which the visual network regarding the chosen research field was built, analysed, and interpreted. The research was based on bibliometrics, which for the elaboration of the study included bibliometrics such as, references, references cited in the field, keywords, author, and institution.

The selection criteria for including the resources required for the analysis were chosen based on the use of the modified coefficient g:

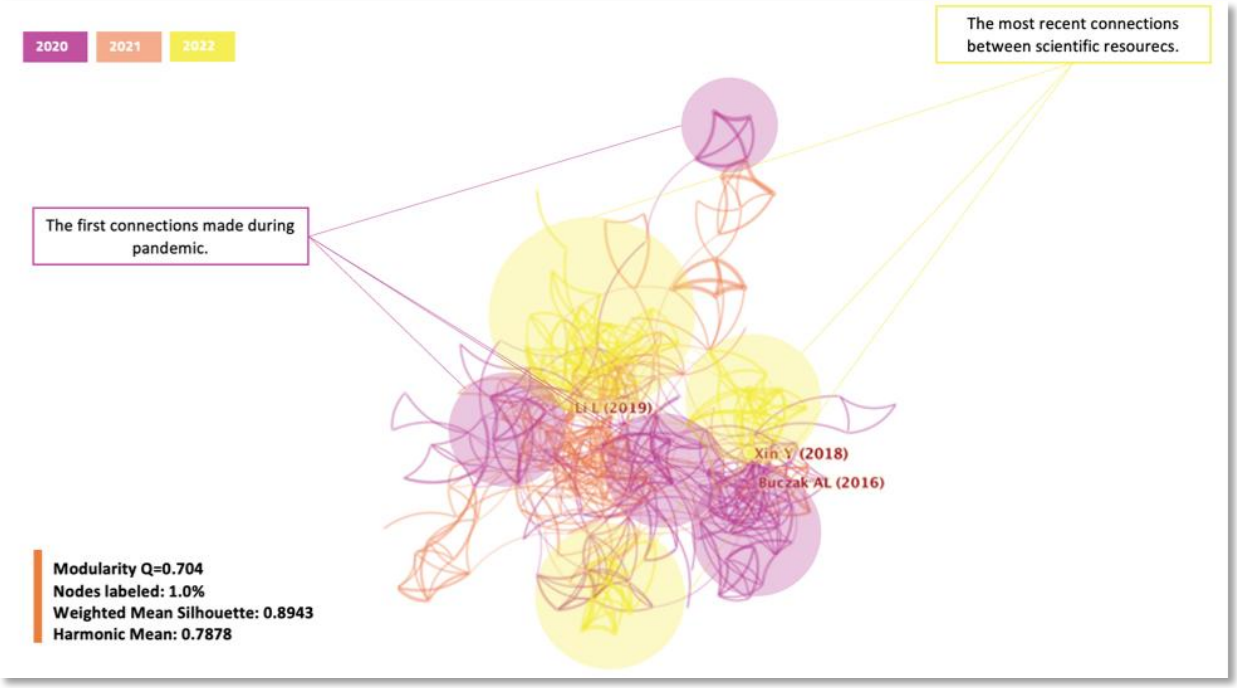
$$g^2 \leq k\Sigma_{i\leq g}c_i, k \in Z^+$$

To include nodes, an increase or decrease in the scale of the factor k=25 was used. Top N levels of most citations represented N=50, and top N% was selected at a level of 10%.

The analysis was applied to the Web of Science database and included 5,287 references published in the period 2020-2022. They were included in the sample based on the relevance criterion. All resources were saved as plain text files and imported into Citespace, version 5.8.R3 for visual network analysis using Java technology.

3. RESULTS

The network created has three colour structures, each corresponding to the year of scientific resources (Fig.1). The figure shows the most recent connections made (yellow) and the first connections made in the pandemic year in the field of cybersecurity. The relevance of the visual network created is shown by the clarity of the decomposition (modularity Q) and the clarity of the configuration of the clusters (silhouette, S) whose values are presented in Table 1.



The most recent connections between scientific resourecs.

The first connections made during pandemic.

Modularity Q=0.704
Nodes labeled: 1.0%
Weighted Mean Silhouette: 0.8943
Harmonic Mean: 0.7878

Fig.1 Visual network on cybersecurity research knowledge

(Source: created by authors with Citespace software)

Table 1: Network metrics

Metric	Value
Modularity (Q)	0.704
Silhouette (S)	0.894

(Source: generated by authors with Citespace software)

What are the major areas of cybersecurity research?

The grouping based on the reference criterion favoured obtaining an answer for the first two critical points formulated previously. In this sense the grouping shows the major clusters according to Fig. 2.

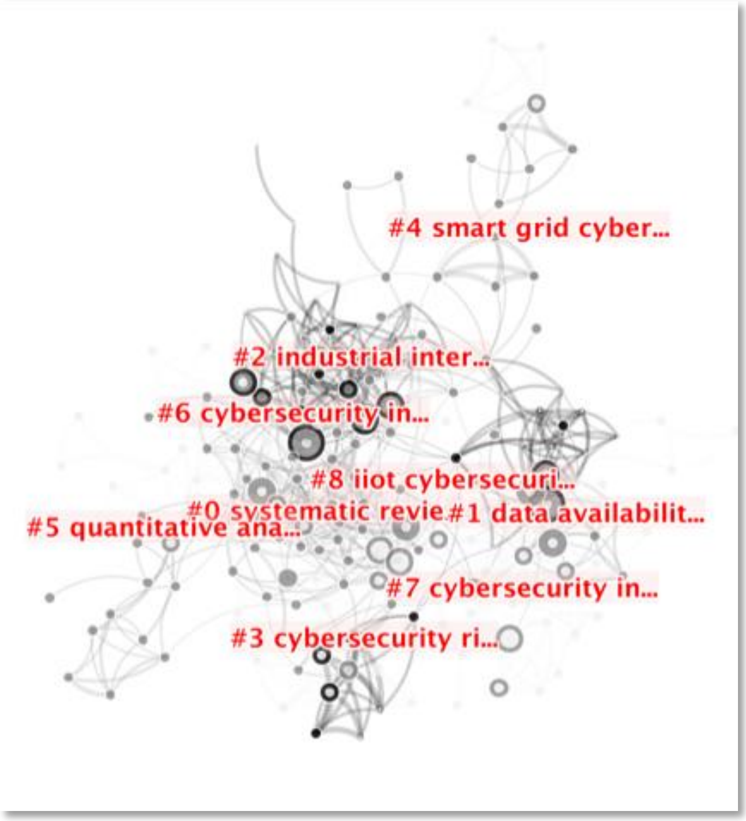


Fig. 2. The larger clusters visualisation

(Source: created by authors with Citespace software)

The largest cluster, rated #0 in the Citespace software, has 40 members, and is labelled as "healthcare organisation" of which Nifakos *et al.* (2021) is the most relevant of the members, with a systematic review of the influence of human factors. on cybersecurity in healthcare organizations.

The second cluster (#1) has 37 members and is labelled by the concept of "learning algorithm", in which Cremer *et al.* (2022) is the most relevant of the members, with a scientific paper such as the systematic review of availability data for cyber risk and cybersecurity.

The third cluster (#2) created (36 members) by the size is labelled with two concepts, namely "cybersecurity awareness" and "cybersecurity response exercises". The most relevant reference is Corallo *et al.* (2022) with a scientific paper on cybersecurity challenges for 4.0 production systems and assessing the level of impact on the business.

What is the main topic in the field of research?

In order to find out what is the main topic in the field of research, the visual network was created according to the keyword and the author cited. In this case, the largest cluster (# 0) has 20 members and has a value of the profile indicator (s) = 0.905. It is labelled "cyber security governance" and "cyber security regulation". The node is represented by the European Commission with 35 citations (Fig.3). According to the grouping created, the most relevant reference is García Segura (2020), with the scientific work on cybersecurity at European level on human rights challenges.

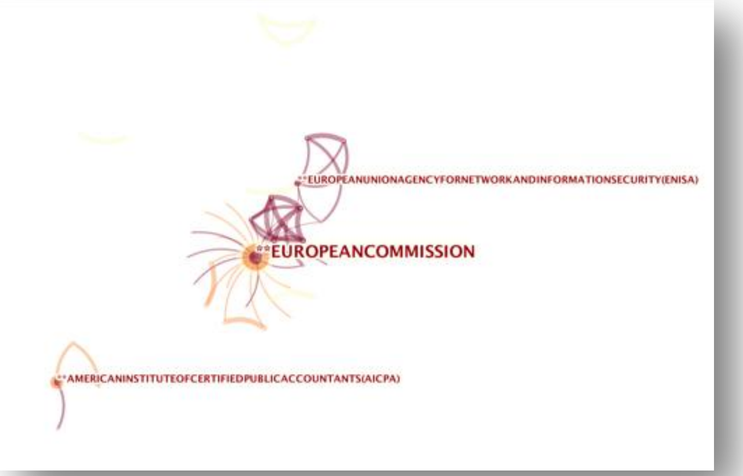
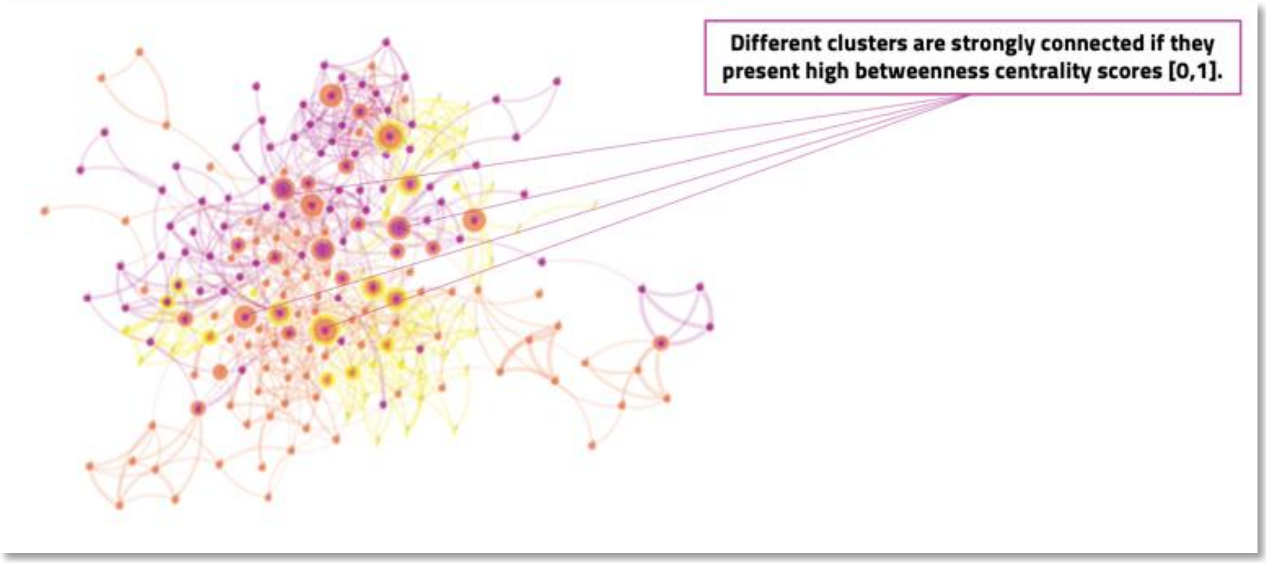

**EUROPEANUNIONAGENCYFORNETWORKANDINFORMATIONSECURITY(ENISA)
**EUROPEANCOMMISSION
**AMERICANINSTITUTEOFCERTIFIEDPUBLICACCOUNTANTS(AICPA)

Fig.3. The node (institution) for the major topic in the research field of cybersecurity (Source: created by authors with Citespace software)

How are major topics connected through specific scientific papers?

In order to find out how major topics are connected through scientific papers, the centrality metric has been interpreted, which can take values between 0 and 1. Different clusters are strongly connected if they have a score as high as possible. In the case of the previously presented node, the value of the indicator is equal to 0.78. In the case of the created network, a high centrality is presented by the nodes highlighted in Fig. 4.



Different clusters are strongly connected if they present high betweenness centrality scores [0,1].

Fig.4. The intersection points of major research topics

(Source: created by authors with Citespace software)

The nodes are represented by the circled references in Fig.5 and named in Fig. 6.

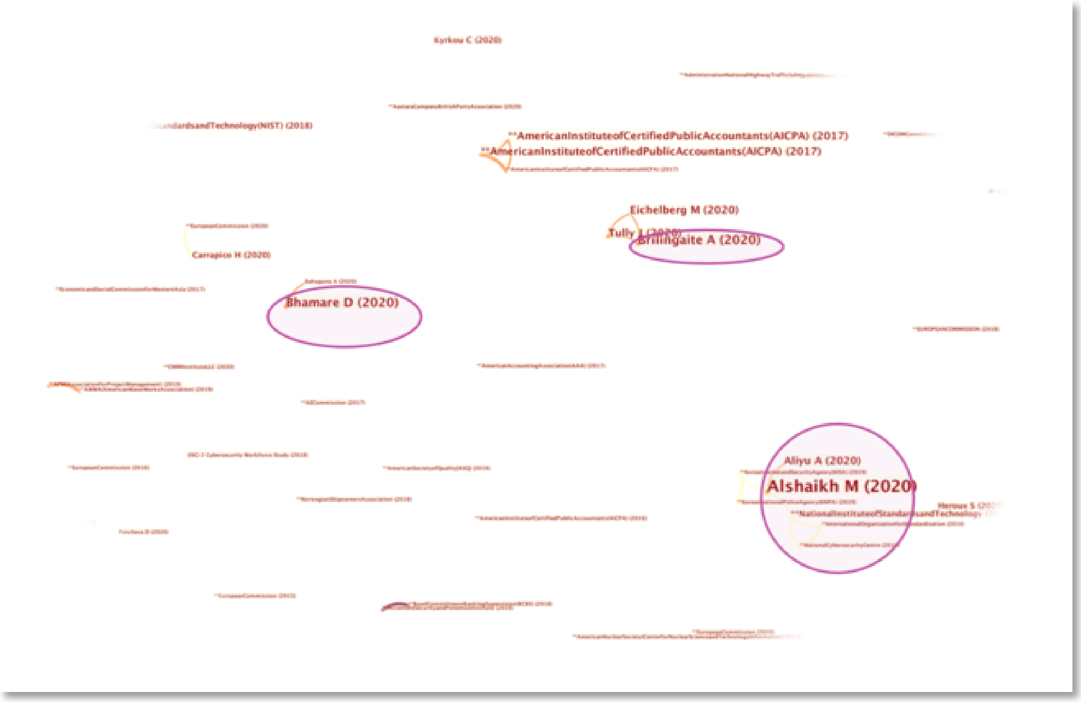
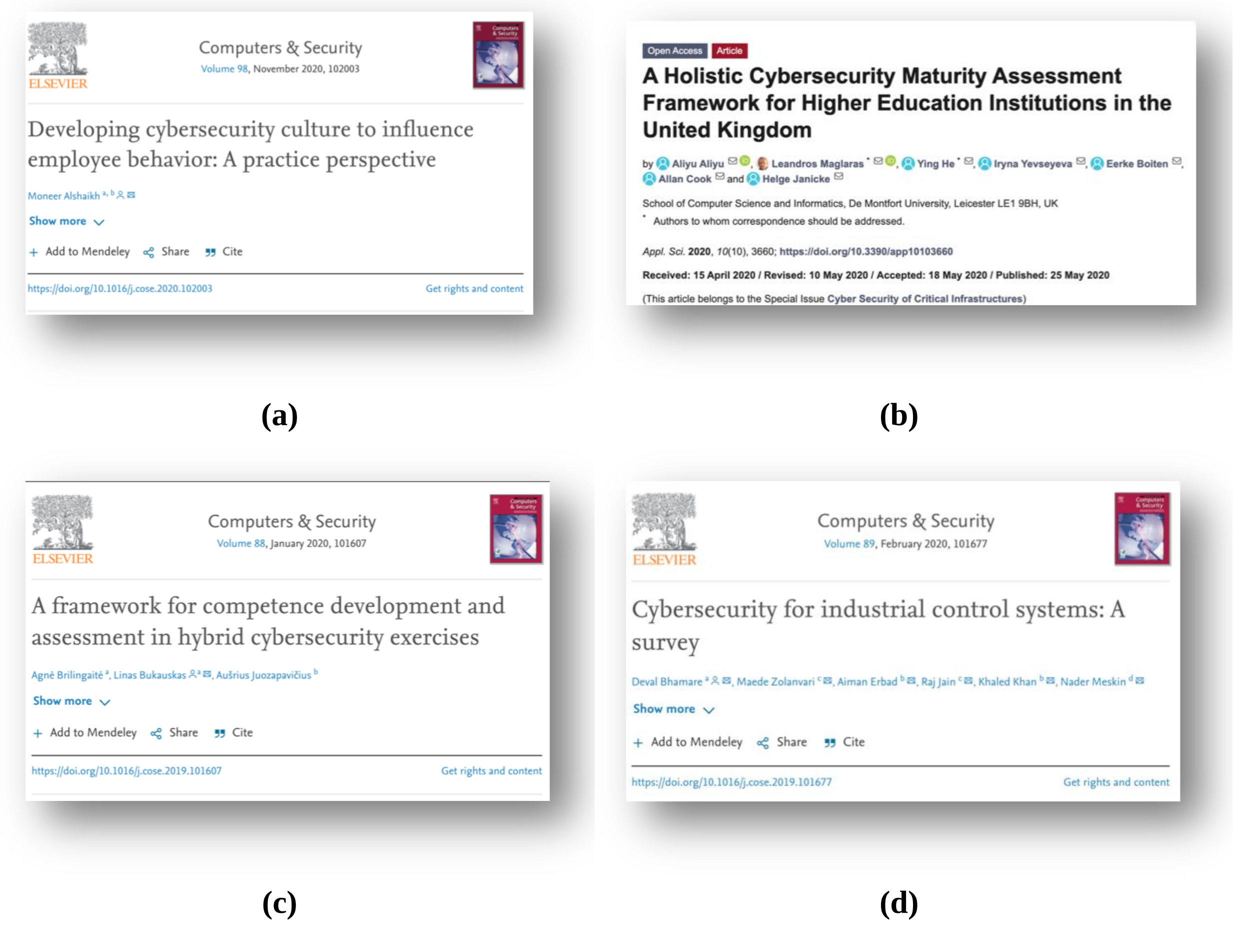

Kyrkou C (2020)
…andardsandTechnology(NIST) (2018)
**AmericanInstituteofCertifiedPublicAccountants(AICPA) (2017)
**AmericanInstituteofCertifiedPublicAccountants(AICPA) (2017)
Eichelberg M (2020)
Tully J (2020)
Brilingaite A (2020)
Carrapico H (2020)
Bhamare D (2020)
Aliyu A (2020)
Alshaikh M (2020)
Herous S (2020)
**NationalInstituteofStandardsandTechnology

Fig.5. The reference of major research topics (nodes)

(Source: created by authors with Citespace software)



ELSEVIER

Computers & Security
Volume 98, November 2020, 102003

Developing cybersecurity culture to influence employee behavior: A practice perspective

Moneer Alshaikh [a, b] ✉

Show more

+ Add to Mendeley Share Cite

https://doi.org/10.1016/j.cose.2020.102003 Get rights and content

(a)

Open Access Article

A Holistic Cybersecurity Maturity Assessment Framework for Higher Education Institutions in the United Kingdom

by Aliyu Aliyu ✉, Leandros Maglaras * ✉, Ying He * ✉, Iryna Yevseyeva ✉, Eerke Boiten ✉, Allan Cook ✉ and Helge Janicke ✉

School of Computer Science and Informatics, De Montfort University, Leicester LE1 9BH, UK

* Authors to whom correspondence should be addressed.

Appl. Sci. **2020**, *10*(10), 3660; https://doi.org/10.3390/app10103660

Received: 15 April 2020 / Revised: 10 May 2020 / Accepted: 18 May 2020 / Published: 25 May 2020

(This article belongs to the Special Issue Cyber Security of Critical Infrastructures)

(b)

ELSEVIER

Computers & Security
Volume 88, January 2020, 101607

A framework for competence development and assessment in hybrid cybersecurity exercises

Agnė Brilingaitė [a], Linas Bukauskas [a] ✉, Aušrius Juozapavičius [b]

Show more

+ Add to Mendeley Share Cite

https://doi.org/10.1016/j.cose.2019.101607 Get rights and content

(c)

ELSEVIER

Computers & Security
Volume 89, February 2020, 101677

Cybersecurity for industrial control systems: A survey

Deval Bhamare [a] ✉, Maede Zolanvari [c] ✉, Aiman Erbad [b] ✉, Raj Jain [c] ✉, Khaled Khan [b] ✉, Nader Meskin [d] ✉

Show more

+ Add to Mendeley Share Cite

https://doi.org/10.1016/j.cose.2019.101677 Get rights and content

(d)

Fig. 6. Scientific resources linking major cybersecurity topics (a) cluster # 0, 8 citations; (b) cluster # 0, 8 citations; (c) cluster # 2, 4 citations; (d) cluster # 12, 4 citations.

(Source: Alshaikh, M. (2020), Brilingaitė, Bukauskas and Juozapavičius (2020), Aliyu, Maglaras, *et al.* (2020) and Bhamare *et al.* (2020)

The results of the comprehensive review of the literature on this field of research show the importance of the human factor in relation to technological adoption in the post-pandemic context. Cybersecurity challenges and solutions also address areas such as human resources, e-commerce, and information technology.

DISCUSSION

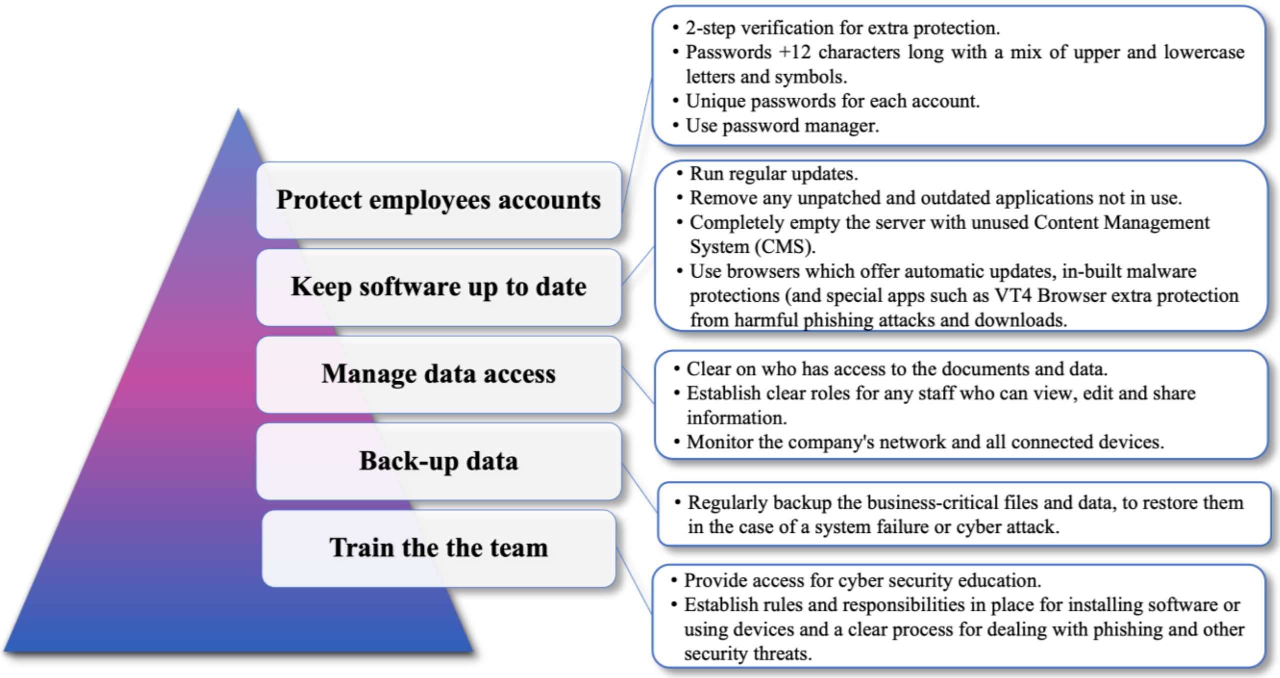
The scientific contribution determine the summary of cybersecurity research knowledge appearing in the academic environment with a new and fresh perspective, presenting the most recent papers published in the field and the intensity of popularity of the paper published in the pandemic year.

The results increase the value of the above-mentioned references due to the integration in the network of the most relevant scientific papers.

The analysis performed confirms the concerns of the academia by discovering the healthcare organisation, cyber risks and cybersecurity awareness labels as being the major areas of cybersecurity research. Furthermore, the study adds the learning algorithm, human factor, cybersecurity governance and cybersecurity regulation as important and relevant topics for the knowledge field.

Moreover, the most relevant papers in 2020-2022 timespan present the concept of developing a cybersecurity culture aiming to influence the behaviour of the employees, the perspective of developing competences, level-up the cybersecurity maturity in higher education and the development of the field in industrial control systems.

To present a more valuable research paper, the authors found some recommendation (Google Digital Garage, 2019) for digital business by increasing the cybersecurity awareness, by develop the culture of the employee in this field and by increasing the degree of protection against this type of risks. The summary is presented in Fig. 7.



- 2-step verification for extra protection.
- Passwords +12 characters long with a mix of upper and lowercase letters and symbols.
- Unique passwords for each account.
- Use password manager.

- Run regular updates.
- Remove any unpatched and outdated applications not in use.
- Completely empty the server with unused Content Management System (CMS).
- Use browsers which offer automatic updates, in-built malware protections (and special apps such as VT4 Browser extra protection from harmful phishing attacks and downloads.

- Clear on who has access to the documents and data.
- Establish clear roles for any staff who can view, edit and share information.
- Monitor the company's network and all connected devices.

- Regularly backup the business-critical files and data, to restore them in the case of a system failure or cyber attack.

- Provide access for cyber security education.
- Establish rules and responsibilities in place for installing software or using devices and a clear process for dealing with phishing and other security threats.

CONCLUSIONS

The information society and the great challenges that digital organisation will face in the digital future offer the opportunity to demonstrate strong resilience and sustainable development, at least in the light of the elements addressed above.

The concern for cybersecurity, a major challenge of the moment, reveals the need to provide support for companies that do not know the field, but are aware of the risks involved in carrying out the activity.

All the results obtained by the research fulfil the purpose of identifying and promoting challenges and opportunities for digital organizations within cybersecurity knowledge field.

With major implication of the academic environment, cyber risks can be diminished, by knowing the circumstances of a constantly evolving field, especially in the scientific literature. Universities and researchers may consider the results obtained through the analysis performed in order to train specialists in the field, but also to advice the top management from targeted digital organizations.

On the other hand, the private sector may fruitful the outcomes of the study by deploying internal rules and procedures to develop a cybersecurity culture, and to prepare the employees to prevent cyber risks.

The future research directions can represent quantitative research to measure the perception of managers regarding the necessity of cyber security assets, trainings, and tools for their business development.

CONFLICTS OF INTEREST AND PLAGIARISM: The authors declare no conflict of interest and plagiarism.

REFERENCES

1. Al-Sanjary, O. I. *et al.* (2022) 'Challenges on Digital Cyber-Security and Network Forensics: A Survey', *Lecture Notes on Data Engineering and Communications Technologies*, 127, pp. 524–537. doi: 10.1007/978-3-030-98741-1_43.
2. Aliyu, A., Maglaras, L., *et al.* (2020) 'A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom', *Applied Sciences*

(Switzerland), 10(10). doi: 10.3390/APP10103660.

3. Aliyu, A., He, Y., *et al.* (2020) ‘Cyber Security Decision Making Informed by Cyber Threat Intelligence (CYDETI) : IEEE CNS 20 Poster’, in *2020 IEEE Conference on Communications and Network Security, CNS 2020*. doi: 10.1109/CNS48642.2020.9162162.
4. Alshaikh, M. (2020) ‘Developing cybersecurity culture to influence employee behavior: A practice perspective’, *Computers and Security*, 98. doi: 10.1016/J.COSE.2020.102003.
5. Annarelli, A. and Palombi, G. (2021) ‘Digitalization capabilities for sustainable cyber resilience: a conceptual framework’, *Sustainability (Switzerland),* 13(23). doi: 10.3390/su132313065.
6. Baltezarevic, R. and Baltezarevic, I. (2021) ‘The Dangers and Threats that Digital Users Face in Cyberspace’, *IPSI BGD TRANSACTIONS ON INTERNET RESEARCH*, 17(1, SI), pp. 46–52. Available at: https://www-webofscience-com.am.e-nformation.ro/wos/woscc/full-record/WOS:000599526900009 (Accessed: 10 June 2022).
7. Bhamare, D. *et al.* (2020) ‘Cybersecurity for industrial control systems: A survey’, *Computers and Security*, 89. doi: 10.1016/J.COSE.2019.101677.
8. Brilingaitė, A., Bukauskas, L. and Juozapavičius, A. (2020) ‘A framework for competence development and assessment in hybrid cybersecurity exercises’, *Computers and Security*, 88. doi: 10.1016/J.COSE.2019.101607.
9. Chen, C. (2010) ‘CiteSpace: Visualizing patterns and trends in scientific literature’, *Retrieved January*, p. 2010. Available at: http://cluster.cis.drexel.edu/~cchen/citespace/ (Accessed: 11 June 2022).
10. Corallo, A. *et al.* (2022) ‘Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review’, *Computers in Industry*, 137. doi: 10.1016/J.COMPIND.2022.103614.
11. Cremer, F. *et al.* (2022) ‘Cyber risk and cybersecurity: a systematic review of data availability’, *Geneva Papers on Risk and Insurance: Issues and Practice*. doi: 10.1057/S41288-022-00266-6.
12. Du, L. *et al.* (2020) ‘A summary of the development of cyber security threat intelligence sharing’, *International Journal of Digital Crime and Forensics*, 12(4), pp. 54–67. doi: 10.4018/IJDCF.2020100105.

13. García Segura, L. A. (2020) 'European cybersecurity: Future challenges from a human rights perspective', *Advanced Sciences and Technologies for Security Applications*, pp. 35–46. doi: 10.1007/978-3-030-12293-5_3.
14. Gladman, I. (2021) 'European Economic and Social Committee (EESC)', in *The European Union Encyclopedia and Directory 2022*, pp. 375–379. doi: 10.4324/9781003179887-1313.
15. Glänzel, W. *et al.* (2019) *Springer Handbook Science and Technology indicators*, *Springer Handbooks*. Available at: https://books.google.ro/books?id=mya7DwAAQBAJ&pg=PA163&lpg=PA163&dq=visualization+of+a+network,+using+Java+technology+citespace&source=bl&ots=xByQPeAf5Z&sig=ACfU3U2KLW--0hsTKK_OZfnMY5BXEWxpSw&hl=ro&sa=X&ved=2ahUKEwj0hbvM5aP4AhWN-yoKHQyVD4YQ6AF6BAgiEAM#v=o (Accessed: 11 June 2022).
16. Google Digital Garage (2019) *Google Digital Garage - Introduction to Content Marketing*. Available at: https://learndigital.withgoogle.com/digitalgarage/course/introduction-to-cybersecurity (Accessed: 11 June 2022).
17. Hassib, B. and Shires, J. (2022) 'Cybersecurity in the GCC: From Economic Development to Geopolitical Controversy', *Middle East Policy*, 29(1), pp. 90–103. doi: 10.1111/mepo.12616.
18. Jbair, M. *et al.* (2022) 'Threat modelling for industrial cyber physical systems in the era of smart manufacturing', *Computers in Industry*, 137. doi: 10.1016/j.compind.2022.103611.
19. Lehto, M. (2015) 'Cyber security competencies - Cyber security education and research in finnish universities', in *European Conference on Information Warfare and Security, ECCWS*, pp. 179–188. Available at: https://www-webofscience-com.am.e-nformation.ro/wos/woscc/full-record/WOS:000361690600022 (Accessed: 10 June 2022).
20. Martínez, M. H. (2020) 'Feminist cyber-resistance to digital violence: Surviving gamergate', *Debats*, 134(2), pp. 89–106. doi: 10.28939/IAM.DEBATS.134-2.7.
21. Mbelli, T. M. and Dwolatzky, B. (2016) 'Cyber Security, a Threat to Cyber Banking in South Africa: An Approach to Network and Application Security', in *Proceedings - 3rd IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2016 and 2nd IEEE International Conference of Scalable and Smart Cloud, SSC 2016*. Institute

of Electrical and Electronics Engineers Inc., pp. 1–6. doi: 10.1109/CSCloud.2016.18.

22. Nifakos, S. *et al.* (2021) ‘Influence of human factors on cyber security within healthcare organisations: A systematic review’, *Sensors*. MDPI AG. doi: 10.3390/s21155119.
23. Ravidas, D., Pattinson, M. R. and Oliver, P. (2021) ‘Cyber Security in Healthcare Organisations’, in *IFIP Advances in Information and Communication Technology*. Springer Science and Business Media Deutschland GmbH, pp. 3–11. doi: 10.1007/978-3-030-81111-2_1.
24. Spanakis, EG; Bonomi, S; Sfakianakis, S; Santucci, G; Lenti, S; Sorella, M; Tanasache, F. (2020) ‘Cyber-attacks and threats for healthcare - a multi-layer thread analysis-Web of Science Core Collection’, in *42ND ANNUAL INTERNATIONAL CONFERENCES OF THE IEEE ENGINEERING IN MEDICINE AND BIOLOGY SOCIETY: ENABLING INNOVATIVE TECHNOLOGIES FOR GLOBAL HEALTHCARE EMBC’20*. Available at: https://www-webofscience-com.am.e-nformation.ro/wos/woscc/full-record/WOS:000621592206121 (Accessed: 10 June 2022).
25. Stevens, R. *et al.* (2019) ‘Applied digital threat modeling: It works’, *IEEE Security and Privacy*, 17(4), pp. 35–42. doi: 10.1109/MSEC.2019.2909714.
26. Xu, Y. *et al.* (2020) ‘AI customer service: Task complexity, problem-solving ability, and usage intention’, *Australasian Marketing Journal*. doi: 10.1016/j.ausmj.2020.03.005.
27. Zwilling, M. *et al.* (2022) ‘Cyber Security Awareness, Knowledge and Behavior: A Comparative Study’, *Journal of Computer Information Systems*, 62(1), pp. 82–97. doi: 10.1080/08874417.2020.1712269.