6-14-2024

A Cybersecurity Standards and Frameworks Knowledge Graph For The Education Of Sustainable Australian Smaller Businesses

Rosetta Romano
University of Canberra, rosetta.romano@canberra.edu.au

Blooma John
University of Canberra, blooma.john@canberra.edu.au

A CYBERSECURITY STANDARDS AND FRAMEWORKS KNOWLEDGE GRAPH FOR THE EDUCATION OF SUSTAINABLE AUSTRALIAN SMALLER BUSINESSES

TREO Paper – Educational disruptions (and participating in the research development roundtables)

Abstract

Cybersecurity is crucial for safeguarding electronic systems and data, protecting privacy, and upholding individual rights. Smaller businesses, often disadvantaged, face frequent cyber threats due to limited resources. The research presented focuses on improving access to cybersecurity standards through a Knowledge Graph (KG), consolidating key frameworks. While enhancing understanding, the KG requires technical proficiency. Future efforts aim to expand coverage and accessibility. This research aligns with governmental support initiatives and contributes to social sustainability goals by empowering smaller businesses in a digitally connected world.

Keywords: Cybersecurity, Social Sustainability Goals, Knowledge Graph, Cybersecurity Standards and Frameworks.

1 Cybersecurity in a hyper-connected and digitized world

Cybersecurity, as defined by the National Institute of Standards and Technology (NIST), aims to prevent damage to, unauthorized use of, exploitation of, and, if needed, the restoration of electronic information and communications systems and the information they contain in order to strengthen the confidentiality, integrity, and availability of these systems. Cybersecurity is a global contemporary issue that is also called information technology security, and it involves the management and utilization of information technology (IT) (Oruj, 2023). At the same time, cybersecurity is a critical aspect of upholding individual freedom and dignity by securing data and protecting the privacy of individuals (Piccarozzi, et al. 2023). Greater awareness and strong multi-stakeholders are crucial for achieving the Sustainable Development Goals (SDGs) in a hyper-connected and digitized world (Michael, et al. 2019).

Small and medium-sized businesses face more disadvantages than their larger corporate counterparts (Segal, 2022). In Australia, there is a cyber-attack every 10 minutes, and 43% of these attacks target SMEs (Griffiths, 2024). Limited resources and affordability barriers often hinder their ability to implement effective cybersecurity measures (Rawindaran et al. 2023).

2 Cybersecurity Standards and Frameworks Knowledge Graph

Standards and frameworks play a crucial role in regulating and guiding organizations on best practices (Brunsson & Jacobsson, 2002). However, accessing and understanding cybersecurity standards and frameworks can be challenging, especially for smaller businesses (Tam et al. 2021). This research focuses on improving access to cybersecurity standards and frameworks for all Australian businesses. The research also tackles the understandability issues by utilizing a Knowledge Graph (KG) to understand if existing standards and frameworks can address the questions asked by smaller businesses or if new ones addressing their needs require development. A KG uses the Resource Description Framework (RDF) triples of relations between things in a domain, i.e. an ontology, and the data to conduct powerful reasoning impossible for humans to undertake.

Using a Design Science Research (DSR) methodology, researchers at the University of Canberra, in Australia, developed ontologies of the Cybersecurity Standards and Frameworks that would be populated in a Knowledge Graph (KG) by Industry Partners who also funded the work. This KG consolidates various cybersecurity standards and frameworks, making them more accessible to users and thereby addressing the problem of access (Myers & Venable, 2014).

Key standards included in the KG are the NIST 800-53 and 800-171, the International Organization for Standardization/International Electrotechnical Commission ISO/IEC 27001, a standard to manage information security; ISO/IEC 27002, an international standard that guides organizations looking to establish, implement and improve an Information Security Management System; the Australian Cyber Security Centre (ACSC) Mitigation Strategies Maturity Model including the Essential Eight and the United Kingdom (UK) Ministry of Defence Standard 05-138 for Defence Providers. Additionally, it includes the Defence Industry Security Program (DISP), incorporates the Australian Government's Information Security Model (ISM) and utilizes the Data Privacy Vocabulary (DPV).

The KG serves as a comprehensive resource, facilitating a better understanding of existing and applicable cybersecurity standards and frameworks. The research question is, 'How well do existing standards and frameworks address the cybersecurity questions asked by smaller businesses?' Given the disparate nature of smaller businesses, a supplementary research question could be asked to determine whether a set of standards and frameworks could represent smaller business cybersecurity concerns.

Efforts are underway to enhance the KG by including extensions to cover additional standards, for example, the Payment Card Industry Data Security Standard (PCI DSS) and regulations such as the General Data Protection Regulation (GDPR); principles, including the Australian Privacy Principles (APPs); and Legislation for example the Security of Critical Infrastructure Act, 2018 (SOCI).

3 Workshop outcomes

This research contributes to social sustainability goals and strengthens the resilience of smaller businesses in a digitized world. This research aims to bridge the gap between cybersecurity resources

and smaller businesses, aligning with the Australian Government's commitment to supporting accessible support programs.

The Treo should draw out the importance of enhancing cybersecurity knowledge and accessibility by using available resources for smaller businesses. Participants will have an opportunity to discuss the use of existing standards and frameworks in cybersecurity education for smaller businesses.

References

Griffiths, C., (2024). *The Latest 2024 Cyber Crime Statistics* (updated February 2024). URL: https://aag-it.com/the-latest-cyber-crime-statistics/ (Accessed: 5 March 2024).

Kelley, G. (Ed.). (2008). *Selected Readings on Information Technology Management: Contemporary Issues: Contemporary Issues.* IGI Global.

Michael, K., Kobran, S., Abbas, R., & Hamdoun, S. (2019, November). *Privacy, data rights and cybersecurity: Technology for good in the achievement of sustainable development goals.* In 2019 IEEE International Symposium on Technology and Society (ISTAS) (pp. 1-13). IEEE.

Myers, M., & Venable, J. (2014). *A set of ethical principles for design science research in information systems*. Information & Management, 51(6), 801-809.

Oruj, Z., 2023. *Cyber Security: contemporary cyber threats and National Strategies. Distance Education in Ukraine: Innovative, Normative-Legal, Pedagogical Aspects*, (2), pp.100-116.

Piccarozzi, M., Stefanoni, A., Silvestri, C., & Ioppolo, G. (2023). *Industry 4.0 technologies as a lever for sustainability in the communication of large companies to stakeholders.* European Journal of Innovation Management.

Rawindaran, N., Jayal, A., Prakash, E. and Hewage, C., 2023. *Perspective of small and medium enterprise (SME's) and their relationship with government in overcoming cybersecurity challenges and barriers in Wales.* International Journal of Information Management Data Insights, 3(2), p.100191.

Segal, E. *Why Small and Medium-Sized Companies Face More Cyber Challenges Thank Large Ones: Survey*. Forbes, www.forbes.com/sites/edwardsegal (13 July 2022, 12:56 PM).

Tam, T., Rao, A., & Hall, J. (2021). *The good, the bad and the missing: A Narrative review of cyber-security implications for Australian small businesses.* Computers & Security, 109, 102385.Avison, D. E. and Fitzgerald, G. (1995). *Information systems development: Methodologies, techniques and tools*, 2nd Edition. London: McGraw-Hill.