6-30-2024

CYBERSECURITY EDUCATION – ANSWERING THE QUESTIONS THAT SMALLER BUSINESSES ARE ASKING

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

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

CYBERSECURITY EDUCATION – ANSWERING THE QUESTIONS THAT SMALLER BUSINESSES ARE ASKING

Research in Progress

Rosetta Romano, University of Canberra, Australia, Rosetta.Romano@canberra.edu.au
Blooma John, University of Canberra, Australia, Blooma.John@canberra.edu.au

Abstract

Cybersecurity is a global contemporary issue concerning the management and utilization of information technology (IT) (Kelley, 2008). Cybersecurity supports social sustainability goals as it is a frequently used tool for data management to secure data and protect privacy (Piccarozzi, et al. 2023). Cybersecurity is integral in maintaining the freedom and dignity of the individual, and greater awareness and strong multi-stakeholder partnerships are crucial for achieving the Sustainable Development Goals (SDGs) in a hyper-connected and digitized world (Michael, et al. 2019). Cyber threats represent IT leaders' biggest concern (Kappelman et al., 2019). While more big companies are hacked, smaller businesses are attacked more frequently, with one in five small to medium businesses being hacked yearly (Segal, 2022). Smaller businesses report affordability barriers preventing them from accessing technologies, trained cyber security staff, and external security services that can keep their organizations safe from cyber attacks (Cynet, 2022). Access to the Standards and Framework may represent another barrier for smaller businesses. The Australian Government has committed to ensuring that small business support programs are easy to understand and accessible, and that businesses have strong incentives to participate (Department of Home Affairs, 2023). This research attempts to remove the barriers to accessing rich resources in cybersecurity Standards and Frameworks to improve the cybersecurity maturity of smaller Australian businesses. Hence, the research question addressed in this paper is, "How can the Standards and Frameworks be used to educate smaller businesses about cybersecurity?" This research provides a scholarly contribution to support the Australian's Governments commitment to provide understandable and accessible Cybersecurity Standards and Frameworks to educate smaller business.

Keywords: cybersecurity, knowledge graph, education, question answering, smaller businesses

1 Introduction

The National Institute of Standards and Technology (NIST) defines cybersecurity as the prevention of damage to, unauthorized use of, exploitation of, and, if needed, the restoration of electronic information and communications systems and the information they contain to strengthen the confidentiality, integrity, and availability of these systems. Cybersecurity is a global contemporary issue concerning the management and utilization of information technology (IT) (Kelley, 2008). Cybersecurity supports social sustainability goals as it is a frequently used tool for data management to secure data and protect privacy (Piccarozzi, et al. 2023). Cybersecurity is integral in maintaining the freedom and dignity of the individual, and greater awareness and strong multi-stakeholder partnerships are crucial for achieving the Sustainable Development Goals (SDGs) in a hyper-connected and digitized world (Michael, et al. 2019).

Cyber threats represent IT leaders' biggest concern (Kappelman et al., 2019). While more big companies are hacked, smaller businesses are attacked more frequently, with one in five small to medium

businesses being hacked yearly (Segal, 2022). Smaller businesses report affordability barriers preventing them from accessing technologies, trained cyber security staff, and external security services that can keep their organizations safe from cyber attacks (Cynet, 2022). Small businesses represent 97.3%[1] of all Australian businesses. By improving cybersecurity for smaller businesses in Australia, this research could improve cybersecurity for more than all Australian businesses (ABS, 2024). Globally, small and medium businesses represent over 90% of the business population (MYOS, 2023). The potential impact of improving cybersecurity education for smaller businesses can be imagined.

Global regulation increasingly relies on alternatives to legal rules called standards (Kerwer, 2005). Certain certifiers may require following specific standards to maintain compliance and demonstrate that a particular situation is being managed (Brunsson and Jacobsson, 2002). Notwithstanding, in principle, following a standard is voluntary (Brunsson and Jacobsson, 2002). A standard is a rule that others have provided about how to organize, what policies to pursue, what kind of services to offer, or how to design their products (Brunsson and Jacobsson, 2002; Kerwer, 2005). A framework refers to the overall structure to support a system.

2 Research Gap

Rich information exists in Cybersecurity Standards and Frameworks. Still, they are complex, overlapping, and scattered on different websites, and the International Standards ISO/IEC attract annual fees to access them. Access to the Standards and Framework may represent a barrier for smaller businesses. The research also includes Indigenous businesses in this category. In Australia, an Indigenous business must have 51% or greater Indigenous ownership. Microbusinesses are the smallest category of businesses, typically defined by their small number of employees and low revenue or turnover (Gherhes et al., 2016). Small businesses are typically larger than micro businesses but still relatively small regarding employees, revenue, and market reach. Small businesses may have a more formal organizational structure, multiple employees, and a broader customer base (Gherhes et al., 2016). Medium-sized businesses are larger than small businesses but smaller than large corporations (Berisha & Pula, 2015). Limited resources concerning the budget and lack of highly skilled cyber experts to keep up with the rapidly evolving cyber threat landscape, lack of awareness and understanding of cybersecurity risks and the importance of implementing a framework, relying on third-party vendors and suppliers for various services and products and trusting these entities with sensitive data and systems are all different levels of challenges experienced by small and micro businesses today (Tam et al., 2021; Cartwright et al., 2023).

The Australian Government has committed to ensuring that small business support programs are easy to understand and accessible and that businesses have strong incentives to participate (Department of Home Affairs, 2023). This research attempts to remove the barriers to accessing rich resources in cybersecurity Standards and Frameworks and to develop an understanding of questions that are core to smaller businesses and those that are specific to different smaller business sectors. The research is also investigating whether the answers to common questions asked by smaller businesses could be used to improve the cybersecurity maturity of the four in ten Australian small businesses that are not confident in their ability to respond to a cyber threat (Business Foundations, 2024). There is no similar research investigating this research problem, and the researchers suspect this is because the standards and frameworks were not developed by or for smaller businesses.

[1] The Australian Bureau of Statistics (ABS) defines small businesses as those with less than 20 employees (ABS, 2023). This research defines smaller businesses as Indigenous, Micro, Small and Medium businesses with fewer than 200 employees.

If the answers to the questions that smaller businesses are asking about cybersecurity existed in an accessible system developed for or by smaller businesses, then Australian business cybersecurity could be increased. Hence, this paper addresses the research question***, "How can a Knowledge Graph be used to educate smaller businesses about cybersecurity?"***

3 Research Methodology

To address the research gap and answer the research question, the research team worked with Industry – Surround Australia Pty Ltd, and Pathfinders Ltd, to develop a Cybersecurity Standards and Frameworks Knowledge Graph (KG). A KG is a multi-relational graph composed of entities as nodes and relations as different types of edges (Wang et al., 2014). This KG aims to provide access to information in applicable Cybersecurity Standards and Frameworks by small Australian businesses. While the research has an Australian focus, it is generalizable to smaller businesses globally that are experiencing the same cybersecurity issues. Thus, there is a need to design and evaluate a Cybersecurity Knowledge Graph (CKG) and a supporting Frequently Asked Questions (FAQ) system (John et al., 2016) that smaller business sectors can access to improve Cybersecurity posture. The research methodology is Design Science Research (DSR), which involves designing and evaluating artifacts, such as new software, processes, algorithms, or systems intended to improve or solve an identified problem (Myers & Venable, 2014).

There are many cybersecurity standards and frameworks available globally and locally, and organizations can choose the ones that best fit their needs. While their specific needs may be different, this research determines whether all smaller businesses are asking common cybersecurity questions. The research, therefore, requires the building of two artefacts. Firstly, a cybersecurity KG (CKG) provides a repository of information available to Australian businesses. The CKG requires technical expertise to develop, maintain, query, and modify it. Secondly, a Q&A system user interface will allow smaller businesses to access the information without requiring technical prowess to query the CKG.

This KG includes the following cybersecurity standards:

1. NIST Framework consists of standards, guidelines, and best practices to manage cybersecurity risk. NIST was developed by the National Institute of Standards and Technology (NIST) in the United States (Shen, 2014).

2. ISO/IEC 27001 - The ISO/IEC 27001 standard enables organizations to establish an information security management system, apply a risk management process adapted to their size and needs, and scale it as necessary as these factors evolve (Humphreys, 2016).

3. ISO 27002 - The ISO 27002 standard is a collection of information security guidelines intended to help an organization implement, maintain, and improve its information security management. While ISO 27001 is the standard for international information security management, ISO/IEC 27002 is a supporting standard that guides how information security controls can be implemented (ISO/IEC, 2022).

4. Australian Cyber Security Centre Essential 8—In 2017, the Australian Cyber Security Centre published the Essential Eight Maturity Model. The four levels of maturity identified within the Essential 8 help organizations implement controls based on their business model (ACSCE, 2017).

Also, the KG includes the Australian Government's Information Security Model and the Essential Eight frameworks. In addition to these Standards and Frameworks, the KG incorporates the Data Privacy

Vocabulary (DPV). DPV is a controlled vocabulary from W3C (available in SKOS and/or OWL) that is well maintained and includes a structure for concepts to do with data protection, privacy, risk, security and a number of other high-level concepts that are useful for document annotation, representing policy, and representing rules (Pandit et al. 2019).

Following the DSR methodology (Myers & Venable, 2014), the design and build of the KG were executed using the Stardog Enterprise Knowledge Graph Platform, as illustrated in Figure 1. Extensions to the KG are currently being investigated. These extensions include the Payment Card Industry Data Security Standards (PCI DSS), the Australian Energy Sector Cyber Security Framework, the General Data Privacy Regulation (GDPR) and the Australian Privacy Principles (APP). Technical users are being engaged in evaluating the design and development of the KG. To avoid overburdening users with technical information, a Frequently Asked Questions (FAQ) online system (John et al., 2016) captures the questions that smaller businesses are asking about cybersecurity. This FAQ provides the user interface to the rich information held in the KG to record the questions and publish the answers in a simple language that is understandable and accessible for smaller businesses. The FAQ system will be available as an educational resource for smaller businesses.

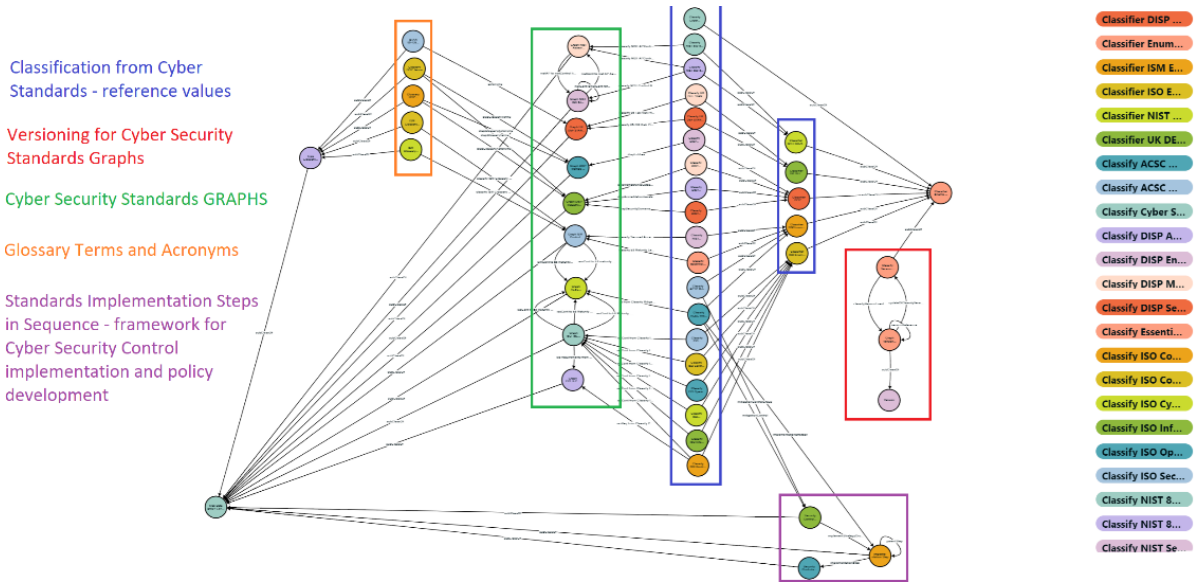

Figure 1. Cybersecurity Standards and Framework Knowledge Graph

There are three stages in this research, as shown in Figure 2. In Stage I, the CKG is developed from the cybersecurity standards and frameworks that apply to all Australian businesses. In Stage II, interviews are conducted with representatives from smaller businesses to determine the questions they are asking about cybersecurity. In Stage III, the researchers search for answers from the CKG and publish these in an FAQ system to educate all smaller businesses.

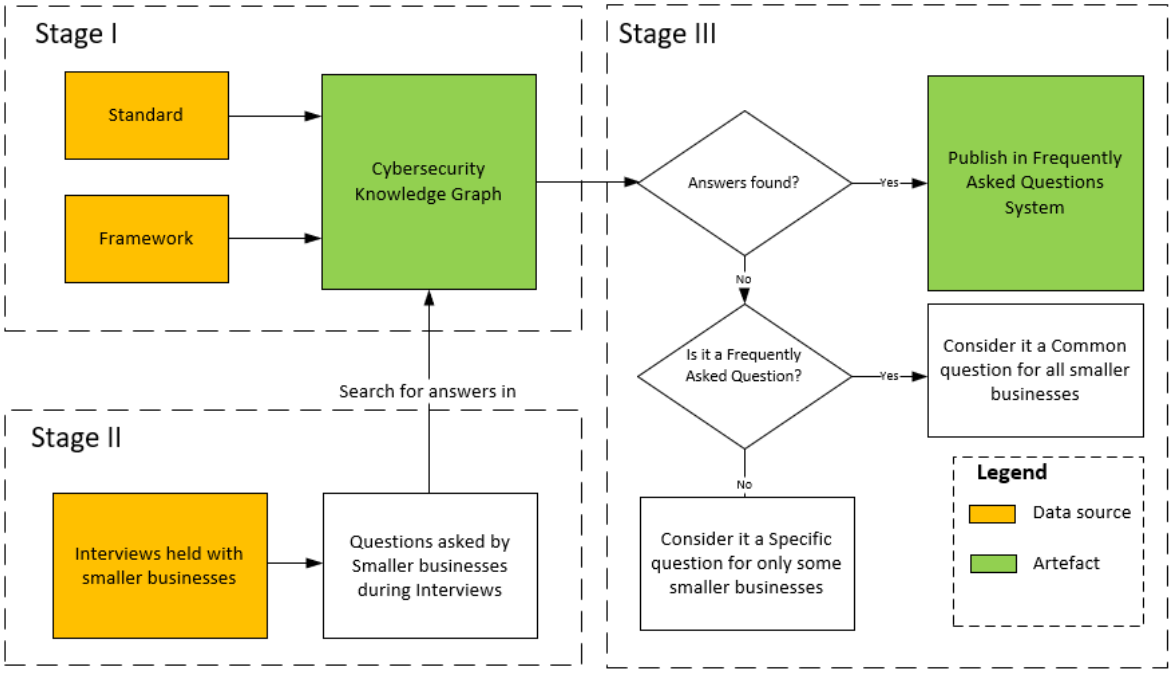

Figure 2. Building a Cybersecurity Knowledge Graph for Educating Smaller Australian Businesses

4 Conclusion and Future Work

As a design-and-build experiment, the CKG explicitly describes relationships between the standards and frameworks. Technical expertise is required to evaluate the relationships in the CKG. However, smaller businesses may only understand how connections between the frameworks and standards can be visualised; they need a more comprehensive question-answering system to help them comprehend the standards and frameworks.

An FAQ system will provide education to smaller businesses by focusing on the questions that they are asking about cybersecurity. In accordance with an ethics application approval[2], smaller businesses are interviewed and asked what questions they have about cybersecurity. So far, it is not surprising that the questions that smaller businesses are asking cannot be found in the many cybersecurity standards and frameworks that apply to all businesses in Australia. Questions such as: What is cybersecurity? What information does my business need to protect? and Why would anyone be interested in my smaller business?

This research provides a scholarly contribution to support the Australian Government's commitment to providing understandable and accessible Cybersecurity Standards and Frameworks for smaller businesses. It also supports social sustainability goals and is integral to maintaining the freedom and dignity of the individual. Greater awareness and strong multi-stakeholder partnerships are crucial for achieving the Sustainable Development Goals (SDGs) in a hyperconnected and digitized world. The research also represents a scholarly examination of a real-world issue facing smaller businesses and a

[2] Ethics Application Number University of Canberra HERC 202313303 24 July 2023.

practical contribution to its commitment to ensuring that support programs are easy to understand and accessible and provide strong incentives to participate in sustainable cybersecurity education to improve the outcomes for smaller businesses, and in turn, for over 97.3% of all Australian businesses.

References:

Australian Bureau of Statistics, July 2019 – June 2023, https://www.abs.gov.au/statistics/economy/business-indicators/counts-australian-businesses-including-entries-and-exits/latest-release.

Brunsson, Nils, and Bengt Jocobsson, (2010). *'Following Standards'*, A World of Standards (Oxford, 2002; online edn, Oxford Academic, 1 Jan. 2010).

Business Foundations, News. 4 in 10 Australian Small Businesses Are Not Confident In Their Ability To Respond To A Cyber Threat. April 12, 2024. https://businessfoundations.com.au/4-in-10-australian-small-businesses-are-not-confident-in-their-ability-to-respond-to-a-cyber-threat/

Cartwright, A., Cartwright, E., & Edun, E. (2023). Cascading information on best practice: Cyber security risk management in UK micro and small businesses and the role of IT companies. *Computers & Security*, 103288.

Cynet, 2022 Survey of CISOs with Small Cyber Security Teams, https://go.cynet.com/2022_ciso_survey (Accessed 1 September 2023)

Department of Home Affairs, 2023. *Cyber Security Strategy 2023-2030*. https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/2023-2030-australian-cyber-security-strategy

Ellery, L., Spencer, J., Ambrose, C., Curtin, C., Kose, K., Sworek, N., and Hutto, Z.' Market Guide for Third-Party Risk Management Solutions' Gartner. ID G00782545. Foley & Hunter, 2013

Foley, D. (2013) "Jus Sanguinis: The root of contention in determining what is an Australian Aboriginal business", Indigenous Law Bulletin, 8(8): 25-29.

Gherhes, C., Williams, N., Vorley, T., & Vasconcelos, A. C. (2016). Distinguishing micro-businesses from SMEs: A systematic review of growth constraints. *Journal of Small Business and Enterprise Development*, *23*(4), 939-963. Berisha & Pula, 2015

Humphreys, E. (2016). *Implementing the ISO/IEC 27001: 2013 ISMS Standard.* Artech house. ISO/IEC 27002:2022 (2022) ISO. Available at: https://www.iso.org/standard/75652.html (Accessed: 19 May 2023).

John, B. M., Chua, A. Y., Goh, D. H. L., & Wickramasinghe, N. (2016). Graph-based cluster analysis to identify similar questions: A design science approach. *Journal of the Association for Information Systems*, *17*(9), 2.

Kappelman, L., Torres, R., McLean, E., Maurer, C., Johnson, V., & Kim, K. (2019). The 2018 SIM IT issues and trends study. MIS Quarterly Executive, 18(1), 51-84

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

Kerwer, D., 2005. Rules that many use: standards and global regulation. *Governance*, *18*(4), pp.611-632.

Mangalaraj, G., Singh, A., & Taneja, A. (2014, August). IT Governance Frameworks and COBIT-A Literature Review. In The Americas Conference on Information Systems.

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.

MYOS. 21 Most Important Small Business Statistics in 2023. https://www.myos.com/en-blog/small-business-statistics.

Pandit, H. J., Polleres, A., Bos, B., Brennan, R., Bruegger, B., Ekaputra, F. J, Fernández, J. D., Hamed, R. G., Kiesling, E., Lizar, M., Schlehahn, E., Steyskal, S. & Wenning, R., Creating a vocabulary for

data privacy: The first-year report of data privacy vocabularies and controls community group (DPVCG). In *On the Move to Meaningful Internet Systems: OTM 2019 Conferences: Confederated International Conferences: CoopIS, ODBASE, C&TC 2019, Rhodes, Greece, October 21–25, 2019, Proceedings* (pp. 714-730). Springer International Publishing.

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.

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

Shen, L. (2014). *The NIST cybersecurity framework: Overview and potential impacts.* Scitech Lawyer, 10(4), 16.

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.

Wang, Z., Zhang, J., Feng, J. and Chen, Z., 2014, June. Knowledge graph embedding by translating on hyperplanes. In *Proceedings of the AAAI conference on artificial intelligence* (Vol. 28, No. 1).