Bull. Aust. Math. Soc. **114** (2026), 566–568
doi:10.1017/S0004972726101968

MAPPING AUSTRALIAN SMALL BUSINESS' PATH TO CYBER-SECURITY BASE CAMP

TRACY TAM

(Received 3 May 2026; first published online 29 September 2026 UTC)

2020 *Mathematics subject classification*: primary 68M25; secondary 68U35.

Keywords and phrases: cyber-security, small business, behavioural barriers, cyber-security human factors.

This thesis investigates the factors holding back security-positive behaviours amongst Australian small businesses and identifies an ideal engagement approach. It then constructs and validates a small business supporting security analysis framework, which is applied to the analysis of four Australian small businesses.

Australian small businesses (<20 employees) are increasingly adopting technology, expanding their exposure to cyber-security risks. The risks have manifested in incidents such as Business Email Compromises (BEC) and scams, impacting the reputation as well as financial and mental well-being of victims [1]. A cyber incident's impact is not isolated to the small business' viability; it puts at risk a small business' value to the community and the customer data it holds. In Australia, small businesses play important roles in the Australian economy, including providing a significant portion of employment [2]. Despite a recognition of cyber-security's importance, there is little evidence of action amongst Australian small businesses to implement cyber-security.

I seek to understand ways to encourage security-positive behaviours amongst Australian small businesses by finding:

(1) an ideal approach for small business to sustainably engage with cyber-security;
(2) a tool/framework to support small business cyber-security analysis;
(3) example security profiles of Australian small businesses.

To maximise impact, this research focuses on sub-20 employee businesses in top employing industries that are Australian Privacy Act exempt, technology and risk management novices and nonfranchisees.

This research was supported through the provision of an Australian Government Research Training Program Scholarship.
Thesis submitted to RMIT University in May 2025; degree approved in 13 September 2025; supervisors Asha Rao and Joanne Hall.

© The Author(s), 2026. Published by Cambridge University Press on behalf of Australian Mathematical Publishing Association Inc.

https://doi.org/10.1017/S0004972726101968 Published online by Cambridge University Press

The initial literature survey [8] highlights that existing research in technology, business and human factors does not provide sufficient focus on the sub-20 employees Australian cohort. As the research discovers, extrapolating results from companies with hundreds of employees potentially introduces human behavioural issues due to an organisation's size. Potential researchers also face difficulties in reaching this cohort. Terminology misalignment and human behavioural bias also adds to the confusion. Systemic factors make Australian small business security action difficult. The lack of technical resources for cyber-security tasks within a small business demands already scarce attention from the small business owner. Informal management styles of small businesses do not align with security industry standards, assumptions of process, documentation and internal skills. The uncertainties within the legal and insurance landscape make risk mitigation strategies unappealing to this cohort.

Due to the central role of a human being in Australian small business cyber-security, I identify an ideal approach for small business owners to engage with cyber-security using scored comparisons against established behavioural frameworks. Three engagement models between small business and cyber-security are analysed: self-protection, product enablement and professional-led intervention. Evaluation of these three models against Protection Motivation Theory [4], Stages of Change [7] and EAST [6], combined with small business challenges, establishes that self-protection was most likely to generate sustainable security engagement and action from small businesses.

A new small business cyber-security posture analysis tool and approach, the Small IT Data (SITD) model [9], is introduced to support the self-protection approach. The SITD model adds a framework for establishing a small business security context using unified modelling language (UML). This approach transforms today's qualitative security analysis process into a structured data model. The SITD model captures the key security concepts and the relationships relevant to a small business. Both nontransient (for example, devices, people, network) and transient (for example, relationships) concepts are captured.

I demonstrate the SITD model's use in three scenarios: business context, technology context and cyber-incident. This is done by modelling two small business profiles and a high profile global malware incident. The SITD model's graphical representations help highlight information gaps useful in cyber-security post-incident reviews and situational analysis.

Two existing small business security audit checklists, the NIST SP 800-37 [5] and NCSC Self Assessment Booklet [3], are used to validate the SITD model. The features of the SITD model are closely examined to ensure Australian small business security challenges are addressed.

Four Australian small business case studies are analysed from three industries: Agriculture, Hospitality and Construction. To minimise human behavioural biases, non-cyber-security-source case studies are obtained from searches of academic repositories and the internet, with the two providing three and one businesses, respectively. Additional context information, triggered by case study discussions, is incorporated where publicly available. The source data was first coded in NVivo as SITD model

https://doi.org/10.1017/S0004972726101968 Published online by Cambridge University Press

objects, before the relationships were drawn in Visual Paradigm. The analysis results in four Australian examples of Australian small business security context profiles. Two of the studies demonstrate the impact external events, outside of the small business' control, have on their security posture.

The research finds cyber-security analysis task sizes nonideal for technology novices, when viewed across all four profiles. All profiles involve a volume of items beyond the ideal capacity of a human's working memory. This observation has implications for the structure of future small business cyber-security endeavours. The analysis produces a list of familiar cyber-relevant concepts that has the potential to help with small business owner's learning and retention of security knowledge.

References

[1] Australian Cyber Security Centre, *Supporting Small Businesses—The ACSC Small Business Cyber Security Guide and Companion Materials* (Australian Cyber Security Centre, Canberra, ACT, 2019).

[2] G. Gilfillan, *Small Business Sector Contribution to the Australian Economy*, Research Paper Series, 2019–2020 (Department of Parliamentary Services, Parliament of Australia, 7 January, 2020).

[3] IASME Consortium, *Cyber Essentials Self-Assessment Preparation Booklet* (National Cyber Security Centre, Malvern, UK, 2022).

[4] J. E. Maddux and R. W. Rogers, 'Protection motivation and self-efficacy: a revised theory of fear appeals and attitude change', *J. Exp. Soc. Psychol.* **19**(5) (1983), 469–479.

[5] National Institute of Standards and Technology, 'Security and privacy controls for information systems and organizations', Technical Report, NIST SP 800-53 Rev. 5 (National Institute of Standards and Technology, Gaithersburg, MD, 2020).

[6] O. Service, *EAST Four Simple Ways to Apply Behavioural Insights* (Behavioural Insights Team, London, 2014).

[7] J. Prochaska, C. Diclemente and J. Norcross, 'In search of how people change: applications to addictive behaviors', *Amer. Psychol.* **47**(9) (1992), 1102–1114.

[8] T. Tam, A. Rao and J. Hall, 'The good, the bad and the missing: a narrative review of cyber-security implications for Australian small businesses', *Comput. Secur.* **109** (2021), Article no. 102385.

[9] T. Tam, A. Rao and J. Hall, 'Structuring the chaos: enabling small business cyber-security risks and assets modelling with a UML class model', in: *Information Security in a Connected World, Celebrating the Life and Work of Ed Dawson*, Lecture Notes in Computer Science, 15600 (eds. C. Boyd, R. Safavi-Naini and L. Simpson) (Springer, Cham, 2025), 259–289.

TRACY TAM, School of Science,
RMIT University, 124 La Trobe St, Melbourne, Victoria 3000, Australia
e-mail: tracy.tam@rmit.edu.au

https://doi.org/10.1017/S0004972726101968 Published online by Cambridge University Press