AVPI Policy Briefing

Cyber Readiness: Enhancing Cyber Security Awareness and Capacity Building for SMEs in Vietnam

December 2023

Australian Government
Department of Foreign Affairs and Trade

Australia Vietnam
Policy Institute

RMIT
UNIVERSITY

Australia Vietnam Policy Institute (AVPI)

The AVPI is the first policy institute focused on Australia's relationship with Vietnam, acting as a partnered public policy hub centred around engagement, collaboration and impact.

The AVPI enables and facilitates discussions on strategic and economic issues in the Australia-Vietnam bilateral relationship. Through disseminating the latest research, identifying upcoming trends and sharing practical insights from people with on-the-ground experience, the AVPI helps to advance a cooperative and secure environment for business and investment.

This activity received grant funding from the Department of Foreign Affairs and Trade under the Australia-Vietnam Enhanced Economic Engagement Grant Program 2021.

Vietnam Sectoral Dialogues

Roundtables Series

Cyber Readiness: Enhancing Cyber Security Awareness and Capacity Building for SMEs in Vietnam

There are several challenges that small and medium-sized enterprises (SMEs) face in Vietnam concerning cyber security. However, this highlights the ongoing and potential collaborative efforts between Australia and Vietnam to address SMEs' cyber security challenges. This policy brief offers recommendations for improving these enterprises' cyber security awareness and capacity building.

In Vietnam, SMEs are enterprises (with a couple of industry exceptions) whose average number of employees contributing to social insurance does not exceed 200 per year, and they either have a total investment capital that is not more than VND100 billion (about AUD6.4 million) or a previous year's total revenue of not more than VND300 billion.[1]

KEY THEMES

1 Library of Congress, "Vietnam: Support for Small and Medium-Sized Enterprises." Global Legal Monitor, Library of Congress, July 18, 2017, accessed May 15, 2023, https://www.loc.gov/item/global-legal-monitor/2017-07-18/vietnam-support-for-small-and-medium-sized-enterprises.

Cyber security Landscape for SMEs in Vietnam

As the digital landscape continues to evolve, cyber security has become a crucial aspect of economic growth and prosperity for countries worldwide.

Vietnam's rapidly expanding digital ecosystem offers numerous opportunities and exposes organisations to a myriad of cyber threats. In 2022, computer viruses cost organisations VND21.2 trillion (approximately AUD1.3 billion) to Vietnamese organisations.[2] Acknowledging the significance of a secure digital environment, the Vietnamese Government has designated cyber security as a national priority, and the country has undertaken substantial measures to bolster its cyber security capacity.[3] Considerable work remains, particularly within the small and medium-sized enterprise (SME) sector, which comprises over 97 per cent of Vietnam's total enterprises.[4]

Cyber security incidents are commonplace nowadays, and SMEs are especially vulnerable targets.[5] According to the National Cyber Security Centre of Vietnam, the number of cyberattacks has increased by approximately 20 per cent year-on-year.[6] While Vietnamese organisations tend to be slightly ahead of their global counterparts on the Cisco Cyber security Readiness Index, 92 per cent of security leaders in Vietnam believe that cyber security incidents are likely to disrupt their businesses over the next 12 to 24 months, 10 percentage points higher than their global peers.[7]

SMEs frequently confront distinctive challenges in addressing cyber security, including limited resources, inadequate awareness, and insufficient access to expertise. Many SMEs in Vietnam are not "cyber-ready", lacking the ability to recognise and manage cyber risks, leaving them susceptible to attacks that could disrupt their operations and inflict lasting damage on their reputation and financial stability.

> "No estimate has been made, but each time an incident occurs, the handling cost is high (about 30-40 million VND per day). In one year, there are around 1-2 incidents, so it's VND50-100 million per year."
>
> **– Edutech Vietnamese SME**

2. Bkav, "Vietnam cyber security overview in 2022 and predictions for 2023", Bkav Security Solutions, 2022, accessed April 26, 2023, https://www.bkav.com/top-new/-/view-content/1468938/vietnam-cyber-security-overview-in-2022-and-predictions-for-2023.

3. Ministry of Information and Communications, "National Cyber security and Safety Strategy: 2025-2030", Vietnam Government, 2022.

4. General Statistics Office of Vietnam, "Statistical Yearbook of Vietnam 2021", Vietnam Government, 2022, accessed 20 April 2023, https://www.gso.gov.vn/wp-content/uploads/2022/08/Sach-Nien-giam-TK-2021.pdf.

5. Max van Haastrecht, Injy Sarhan, Alireza Shojaifar, et al. "A Threat-Based Cyber security Risk Assessment Approach Addressing SME Needs", 16th International Conference on Availability, Reliability and Security, 2021.

Considering the pivotal role played by SMEs in Vietnam's economy and the escalating threat of cyber-attacks, policymakers must take proactive measures to enhance cyber security readiness through awareness and capacity building for SMEs. Collaborative efforts to secure the broad adoption of cyber security norms can help promote social and economic development and improve stability. Intentionally developing an Australia-Vietnam partnership in cyber security will seek to strengthen the capacity of Vietnamese SMEs to combat cyber threats, fostering a resilient digital and critical infrastructure ecosystem that benefits both nations. By leveraging Australia's expertise and experience in this domain, this partnership can promote a robust and secure digital environment in Vietnam, ultimately reinforcing the broader Australia-Vietnam relationship.[8]

> "...cyberspace and critical technology affect all aspects of international relations." – Australia's International Cyber and Critical Tech Engagement Strategy, Department of Foreign Affairs and Trade, (p.12)
>
> **– Edutech Vietnamese SME**

Key Takeaways

- The rapid growth of Vietnam's digital economy and increasing cyber threats make it essential to prioritise cyber security awareness and readiness among SMEs.
- SMEs in Vietnam face significant challenges in recognising and addressing cyber threats, including a lack of resources, technical expertise, and awareness of cyber security risks.
- Capacity building programs, informed by self-assessment tools such as train-the-trainer initiatives and digital resource centres, can effectively improve cyber security awareness and practices among SMEs.
- Collaboration among policymakers, businesses, and other stakeholders is crucial in creating a resilient digital ecosystem that supports the growth and development of SMEs in Vietnam.

6 Ministry of Information and Communications, "Cyber attacks rise in Vietnam", Vietnam Government, 2022, accessed 21 April 2023, https://english.mic.gov.vn.

7 ICisco, "Cisco Cyber security Readiness Index: Resilience in a Hybrid World", Cisco, 2023.

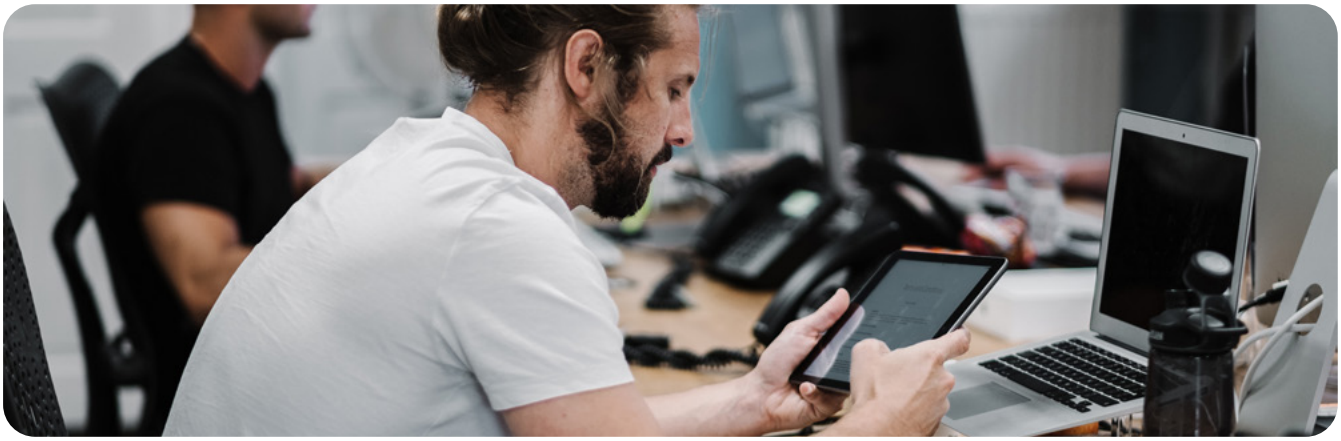
8 Michael Raska and Benjamin Ang, "Cyber security in Southeast Asia", Asia Centre, 2018, accessed April 25, 2023, https://asiacentre.eu/wp-content/uploads/2021/11/NotePresentation-AngRaska-Cyber security_180518.pdf.

Enhancing Cyber Security Awareness for SMEs in Vietnam

Vietnam's rapid economic growth and increasing adoption of digital technologies have made it an appealing target for cybercriminals. Consequently, cyber security assurance is becoming an increasingly integral aspect of maintaining business operations and attracting investment. Raising awareness about cyber threats and risks is essential, particularly for SMEs that are susceptible to losses and reputational damage under attack.

A study by Cisco shows that SMEs in Asia are more exposed to cyber security threats than before. One in two (56 per cent) SMEs suffered a cyber incident in the past year, with 75 per cent losing critical customer information to malicious actors.[9] Despite the escalating threat, many SMEs in Vietnam lack the requisite knowledge and resources to identify and address cyber threats[10]. In part, this deficiency in cyber security readiness can be attributed to the swift development of the digital economy, low public awareness and understanding of cyber security, and an evolving policy and legislative landscape.

Vietnamese SMEs confront various challenges in recognising and addressing cyber threats. Many SMEs lack the necessary technical expertise and resources to implement robust cyber security measures, such as firewalls, anti-virus software, and intrusion detection systems. Cybercriminals often employ sophisticated techniques like phishing, social engineering, and malware attacks, making it difficult for SMEs to defend themselves.[11] Additionally, SMEs might not prioritise cyber security as they concentrate on other business objectives, such as increasing revenue and expanding their customer base. Raising awareness of the importance of cyber security and offering practical guidance to SMEs are crucial for reducing the risk of cyberattacks. In the 2022 Vietnam SME cyber-fitness survey, 44 per cent of respondents indicated that employee cyber security awareness was "extremely important". Alarmingly, 13 per cent of respondents felt that employee cyber security awareness was not important at all.[12]



9. Cisco, "Cyber security for SMBs: Asia Pacific Businesses Prepare for Digital Defense", Cisco, 2021, accessed April 25, 2023. https://www.cisco.com/c/dam/global/en_sg/products/security/meet-max-report-2021/assets/data/cyber security-for-smbs-asia-pacific-businesses-prepare-for-digital-defense.pdf.https://vietnamnews.vn/economy/1314758/saigon-hi-tech-park-attracts-12b-worth-of-investment-over-2-decades.html.

10. Rebecca Oi, "Cyber security is still challenging for ASEAN businesses", Tech Wire Asia, 2021, Accessed April 25, 2023, https://techwireasia.com/2021/11/cyber security-are-challenging-asean-businesses/.

11. The ASEAN, "Digital Transformation – Issue 23." The ASEAN, 2022, accessed April 25, 2023, https://asean.org/wp-content/uploads/2022/11/Issue-23-Digital-Transformation-digital-version.pdf.

12 . AP Hiep Pham, "2022 Vietnam SME Cyber-Fitness", Centre of Cyber security Research and Innovation, 2022.

Raising public awareness of cyber security is vital for mitigating risks, as human error is often deemed the weakest link in the cyber security chain. 95 per cent of cyber security breaches are attributed to human error.[13] Traditional phishing attacks are among the most prevalent methods of targeting SMEs. This prevalence underscores the effectiveness of exploiting human vulnerabilities when malevolent attacks go unnoticed by owners, operators, or customers.[14] By educating individuals about potential threats and equipping them with knowledge and tools to address these risks, society becomes more resilient against cyberattacks.

> *"Most employees do not recognise the risks. They have not realised the danger of leaking information outside."*
>
> **– Edutech Vietnamese SME**

Automating the communication of cyber security knowledge can help SMEs adopt good cyber security practices.[15] Organising awareness-raising events like public safety campaigns or workshops can be practical for SMEs.[16] These events can provide SMEs with practical guidance on identifying and addressing cyber threats, such as spotting phishing emails or installing security updates. Furthermore, resource portals that offer information on cyber security best practices and practical tools can benefit SMEs lacking the resources to implement robust cyber security measures. Such portals can also provide guidance on cyber security-related legal and regulatory requirements.

As a first step, enhancing cyber security awareness among SMEs is crucial for reducing the risk of cyberattacks and ensuring the sustainability of Vietnam's digital economy. By offering practical guidance through awareness-raising events and resource portals, SMEs can better protect themselves against cyber threats and contribute to building a more resilient and secure digital ecosystem.

13. Paul Mee, and Rico Brandenburg, "After reading, writing and arithmetic, the 4th 'r' of literacy is cyber-risk", World Economic Forum, 2020, accessed April 25, 2023, https://www.weforum.org/agenda/2020/12/cyber-risk-cyber-security-education.

14. Vietnamnet, "Phishing attacks still occurring at the same rate", Vietnamnet, 2022, accessed 22 April, 2023, https://vietnamnet.vn/en/phishing-attacks-still-occurring-at-same-rate-2069989.html.

15. Alireza Shojaifar, Samuel A. Fricker, and Martin Gwerder, "Automating the Communication of Cyber security Knowledge: Multi-Case Study", In Information Security Education: Information Security in Action 2020, 109-122. Springer, 2020..

16. Alireza Shojaifar and Heini Järvinen, "Classifying SMEs for Approaching Cyber security Competence and Awareness", 16th International Conference on Availability, Reliability and Security, 2021.

Cyber-fitness in Australian and Vietnamese SMEs

Initiatives such as the National Survey on Cyber Security Readiness of Vietnamese SMEs conducted by RMIT Vietnam, Vietnam Information Security Association (VNISA), and Vietnam Association for Small and Medium Enterprises (VINASME) are crucial for developing an understanding of the current cyber security readiness and informing tailored responses.[17]

The survey, conducted in 2022, gave a comprehensive view of the state of cyber-fitness for SMEs in Vietnam and offered a comparison point to Australia's "state of cyber fitness in Australian small businesses" conducted in 2021.

> "An understanding of the factors affecting cyber security readiness is crucial to devise appropriate solutions for businesses to improve the current low level of cyber fitness among most SMEs."
>
> **- Dr Pham Cong Hiep**

72 per cent of Australian SMEs considered cyber security "very important" compared to 77 per cent of Vietnamese SMEs considered cyber security "important" or "extremely important". However, 57 per cent of Vietnamese SMEs were confident that they were comfortable with their current level of information security management knowledge and skills compared to less than 50 per cent of Australian SMEs who felt the same way – most feeling they could do more.

While Australian and Vietnamese SMEs consider cyber fitness important, other issues are prioritised and invested in first. This was reflected in that 19 per cent of Australian SMEs spent AUD$0 on cyber security within the previous 12 months. The primary motivating factor for Australian and Vietnamese SME business owners to consider their cyber risk was a direct threat from a cyber incident.[18]

However, some organisations have comprehensive processes to deal with cyber security incidents. One such interviewee outlined their process:

> "It [our cyber security measures] can be divided into two processes: general regulations and project-specific regulations. The company operates with its own management team to ensure the management system and conducts periodic audits. There is a monthly cyber security checklist to check all running projects to implement correctly, protect customer information, etc."
>
> **- Gaming and Entertainment Vietnamese SME**

17. Ngoc Hoang, "Small and medium-sized enterprises approach a cyber-secure future", RMIT, 2022, accessed April 25, 2023, https://www.rmit.edu.vn/news/all-news/2022/jan/small-and-medium-sized-enterprises-approach-a-cyber-secure-future.

18. RMIT, "Big cyber security questions for small business: The state of cyber fitness in Australian small businesses", RMIT, 2021, accessed 17 May 2023, https://cynch.com.au/small-business-cyber-fitness-2021 and AP Hiep Pham, "2022 Vietnam SME Cyber-Fitness", Centre of Cyber security Research and Innovation, 2022..

Developing Cyber Resilience

Building cyber resilience is crucial for small and medium-sized enterprises (SMEs) in Vietnam, given the increasing prevalence and sophistication of cyber threats. SMEs are particularly vulnerable to cyber attacks due to limited resources and technical expertise, making them an attractive target for cybercriminals.[19]

As a result of direct attacks, SMEs in Vietnam feel more apprehensive about cyber security risks, with 71 per cent of the survey respondents in Vietnam indicating that they are now more worried about cyber security threats.[20] The good news is that SMEs are taking incremental steps to invest in their cyber security even if those steps are inadequate to make the sector "cyber ready". Over 87 per cent of Vietnamese SMEs indicated that they had increased their investment in cyber security over the past three years – even if it is only by a few percentage points.[21] Their Australian counterparts shared this attitude.[22] These statistics suggest a growing understanding of the need to become more cyber-resilient. Overwhelmingly and unsurprisingly, Vietnamese SMEs felt an increased need to invest in cyber security and information safety training after an incident or breach occurred.[23]

In a recent World Economic Forum survey conducted with Accenture, 81 per cent of survey respondents believe digital transformation is the primary driver in improving cyber resilience.[24] However, many SMEs may lack the necessary resources and budgets to invest in cyber security infrastructure and personnel, making it challenging to develop and implement effective cyber security strategies. With much focus on large firms and government entities, affordable smaller-scale cyber security solutions tend to be overlooked. This was reinforced in the Australian State of Cyber-fitness report. "The 'business' in small business aligns them to enterprise-level solutions at a sophistication they don't need that comes with a price tag they definitely can't afford. So instead, they now believe expertise to be out of reach."[25]

19. Edward Segal, "Small Businesses Are More Frequent Targets Of Cyberattacks Than Larger Companies: New Report", Forbes, 2022, accessed April 25, 2023. https://www.forbes.com/sites/edwardsegal/2022/03/30/cyber-criminals/?sh=1edc34f352ae.

20. Cisco, "Cyber security for SMEs: Asia Pacific Businesses Prepare for Digital Defense", Cisco, 2021, accessed 22 April 2023.

21. Ahn Duc, "Cisco report on cyberattack threat among Vietnamese SMEs", Vietnam Investment Review, 2021, accessed 22 April 2023, https://vir.com.vn/cisco-report-on-cyberattact-threat-among-vietnamese-smes-88307.html.

22. RMIT, "Big cyber security questions for small business: The state of cyber fitness in Australian small businesses", RMIT, 2021, accessed 17 May 2023, https://cynch.com.au/small-business-cyber-fitness-2021.

23. AP Hiep Pham, "2022 Vietnam SME Cyber-Fitness", Centre of Cyber security Research and Innovation, 2022.

24. World Economic Forum, "Global Cyber security Outlook 2022 Insight Report", WEF, 2022, accessed April 25, 2023, https://www3.weforum.org/docs/WEF_Global_Cyber security_Outlook_2022.pdf.

25. RMIT, "Big cyber security questions for small business: The state of cyber fitness in Australian small businesses", RMIT, 2021, accessed 17 May 2023, https://cynch.com.au/small-business-cyber-fitness-2021.

A multifaceted approach to addressing cybercrime is required in a complicated landscape, and security solutions are one facet. There is an increasing response from the market, with commercial firms set to launch more cyber security products that address cyber security for SMEs.[26] An example is the Kaspersky Endpoint Detection and Response Optimum solution launched in 2021, designed specifically for SMEs to help protect themselves against cybercrimes.[27]

SMEs require cyber resilience capabilities to mitigate the risks and thrive with as little disruption as possible.[28] Only 31 per cent of SME respondents in Vietnam indicated that they undergo general training to raise awareness of cyber security and the ability to identify a cyber security incident.[29] This training is usually undertaken in the workplace.

Capacity building programs can be an effective approach to building cyber resilience among SMEs.[30] One such program is the train-the-trainer program, which aims to develop the capacity of SMEs to recognise and address cyber threats. Through programs like these, one can train SME employees as cyber security trainers, enabling them to train their colleagues on cyber security best practices, tools, and techniques. SMEs can then establish a culture of cyber security within their organisation, reducing their vulnerability to cyber threats.

For SMEs that want to undergo digital transformation but cannot yet drive this independently, there is a rise of the Chief Technology Officer (CTO) or Chief Security Officer (CSO) as-a-service offering that is becoming quickly popular in countries like Singapore. Referred to as "CTOaaS" or "CSOaaS", SMEs can assess their cyber readiness using a self-assessment tool recommending the next steps to increase their cyber security capabilities.[31] There is scope to adopt similar successful government initiatives such as Australia's Cyber Security Assessment Tool, a tool run by the Department of Industry, Science, Energy and Resources, or Singapore's SG Cyber Safe Program, which aims to develop awareness and tailor capacity-building resources and programs.[32] Initiatives like these will provide access to existing resources and global expertise.

A long-term approach will focus on developing the next generation of cyber security capability. AT Kearney sets an urgent call to action by outlining four main areas to concentrate on (1) Developing the next generation of cyber security professionals, (2) Strengthening the local cyber security industry through deeper cooperation and international collaboration, (3) Fostering research and development (R&D) investment around emerging threat vectors, and (4) Anchoring world-class capabilities to facilitate knowledge exchange and capability building.[33]

Building resilience among SMEs in Vietnam is critical to protecting against cyber threats and ensuring their sustainability. Capacity building programs can effectively enhance cyber security awareness and practices among SMEs. With the increasing prevalence of cyber threats, Australia can support SMEs in Vietnam to prioritise cyber resilience and take steps to improve their cyber security posture.

26. Bharath Aiyer, Venky Anant, and Daniele Di Mattia, "Securing small and medium-size enterprises: What's next?", McKinsey & Company, 2021, accessed April 25, 2023, https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/securing-small-and-medium-size-enterprises-whats-next.

27. Vietnam News, "Kaspersky launches new cyber security solution for small and medium sized businesses", Vietnam News (Eng), 2021, accessed 22 April 2023, https://vietnamnews.vn/economy/913131/kaspersky-launches-new-cyber-security-solution-for-small-and-medium-sized-businesses.html.

28. Juan Francisco Carías, Saioa Arrizabalaga, Leire Labaka, and Josune Hernantes, "Cyber Resilience Self-Assessment Tool (CR-SAT) for SMEs", IEEE, 2021.

29. AP Hiep Pham, "2022 Vietnam SME Cyber-Fitness", Centre of Cyber security Research and Innovation, 2022.

30. Robert Collett and Nayia Barmpaliou, "International Cyber Capacity Building: Global Trends and Scenarios", European Union Institute for Security Studies, 2021, accessed April 25, 2023, https://www.iss.europa.eu/sites/default/files/EUISSFiles/CCB%20Report%20Final.pdf.

31. GoBusiness Singapore & Infocomm Media Development Authority, "CTO-as-a-Service", Infocomm Media, 2023.

32. Department of Industry, Science, Energy and Resources, "Digital Business Tools," Australian Government, accessed April 25, 2023, https://digitaltools.business.gov.au/.

33. AT Kearny, "Cyber security in ASEAN: An urgent call to action", AT Kearny, 2018.

Collaborative Efforts to Improve Cyber Security Norms

The imperative for policymakers, businesses, and other stakeholders to collaborate in enhancing cyber security for SMEs in Vietnam has never been more critical.

Recent advancements in cyber security initiatives demonstrate that cooperation is instrumental in tackling SMEs' challenges when implementing effective cyber security measures. A little under 40 per cent of Vietnamese SME respondents indicated that they were either unsure or did not have cyber security policies in place.[34]

By joining forces, stakeholders can pool resources, exchange expertise, and establish a coordinated strategy to address the multifaceted cyber security landscape. The 2018 ASEAN Leaders' Statement on Cyber Security Cooperation highlighted the need to build closer cooperation among ASEAN Member States and other partner countries on cyber security policy development and capacity building initiatives.[35] A collaborative approach can help forge a more resilient digital ecosystem that benefits all parties involved and bolsters the growth and development of SMEs in Vietnam.

The Department of Foreign Affairs and Trade (DFAT) is committed to providing funding and resources to support initiatives that strengthen cyber security in Vietnam. This commitment is reflected in the Australian Government's International Cyber and Critical Tech Engagement Strategy, which aims to support international collaboration to promote an open, free, and secure cyberspace. The strategy outlines a range of measures Australia is taking to enhance international cyber security cooperation, including initiatives to support capacity building in the Indo-Pacific region.[36]

34. AP Hiep Pham, "2022 Vietnam SME Cyber-Fitness", Centre of Cyber security Research and Innovation, 2022.

35. Department of Foreign Affairs and Trade (DFAT). "Australia's International Cyber and Critical Tech Engagement." Cyber and Critical Tech Cooperation Program. Accessed April 25, 2023. https://www.internationalcybertech.gov.au/.

36. Department of Foreign Affairs and Trade, "International Cyber and Critical Tech Engagement Strategy", 2021, accessed 23 April 2023, https://www.internationalcybertech.gov.au/.

While commitments to change at a government-to-government level lay the foundation for observable impact, the transformative effects within evolutionary economics can be more comprehensively understood through a three-tiered structure: micro-level, which occurs at the individual level; meso-level, encompassing implementation through organisations and institutions, and macro-level, involving government-to-government partnerships and cooperation, a perspective reinforced in an Australia-Vietnam Policy Institute business champions roundtable discussion.[37]

Consequently, for tangible change to occur, individual SMEs must be directly empowered and equipped to undertake the necessary steps to bolster their own cyber resilience. This necessitates fortifying the economic ecosystem at the SME level, which involves educators, advocates, commercial security solution providers, and buyers.

International partnerships play a crucial role in enhancing cyber security for SMEs in Vietnam. These collaborations bring together a diverse array of stakeholders, including policymakers, businesses, and other organisations, to cooperate in developing and implementing cyber security initiatives. Through these partnerships, Vietnamese SMEs can benefit from the expertise, resources, and best practices of international partners.[38]

Furthermore, international partnerships can aid SMEs in Vietnam in overcoming the obstacles they encounter in implementing effective cyber security measures, such as limited resources, skills, and awareness of cyber security risks. By tapping into the expertise and resources of international partners, Vietnamese SMEs can bolster their cyber security resilience and better safeguard their business interests.[39]

In most instances, understanding the cyber security landscape for SMEs and the consequential interventions, whether in Australia or Vietnam, relies on a self-assessment framework. There are few applied formalised impact assessments through structured, independent evaluation frameworks. Some exceptions include New Zealand's Digital Boost. As cyber resilience interventions become more permanent, the inclusion of structured monitoring and evaluation frameworks will need to be embedded within the design of public policies.[40]

The enhancement of cyber security for SMEs in Vietnam necessitates a joint effort from policymakers, businesses, and other stakeholders. Recent collaborative endeavours have demonstrated that international partnerships are an effective means of improving cyber security awareness and capacity building for Vietnamese SMEs. Nevertheless, more must be done, and stakeholders should prioritise cyber security and collaborate to address the challenges faced by SMEs.

37. Kurt Dopfer, John Foster & Jason Potts, "Micro-Meso-Macro", Journal of Evolutionary Economics, (2004).

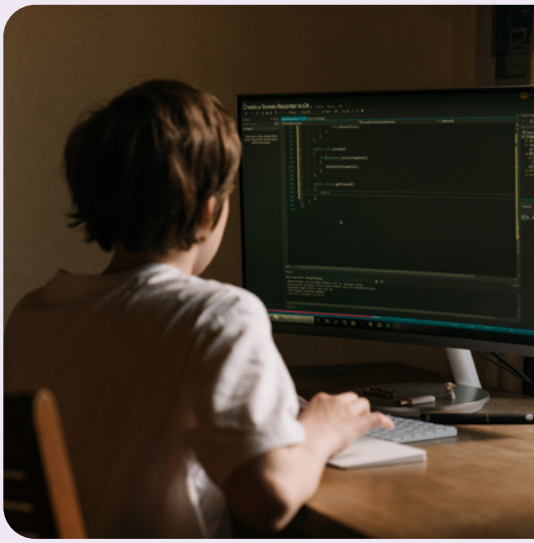
38. AT Kearny, "Cyber security in ASEAN: An urgent call to action", AT Kearny, 2018.

39. Digital McKinsey and Global Risk Practice, "Perspectives on transforming cyber security", McKinsey & Company, 2019.

40. APEC Small and Medium Enterprises Working Group, "What comes after SME Digital Transformation? – Measuring Effectiveness of Public Policy and Identifying Trends for the Post-Digital Era", 2020, accessed April 25, 2023, https://www.apec.org/docs/default-source/publications/2023/4/what-comes-after-sme-digital-transformation/223_sme_what-comes-after-sme-digital-transfromation.pdf.

Emerging Insights

Increasing cyber security across Southeast Asia is crucial for the region's future economic growth and security and the stability of our shared region. Focusing on enhancing cyber resilience for SMEs in Vietnam is vital to ensure the sustainability and development of the nation's digital economy and strengthen the Australia-Vietnam relationship. As SMEs face increasing cyber threats and vulnerabilities, a comprehensive approach that raises awareness, builds capacity, and fosters collaboration among stakeholders is essential.



To see ground-level change occur, we recommend the following:

- Support the development of tailored cyber security solutions and training programs for Vietnamese SMEs that address this sector's specific needs and constraints.
- Encourage and partner with government and industry associations to organise workshops, train-the-trainer programs and resource portals that focus on improving Vietnamese SMEs' technical expertise and understanding of cyber security risks.
- Facilitate international partnerships to bring together stakeholders and resources worldwide to enhance cyber security awareness and capacity building for Vietnamese SMEs.
- Establish resource portals and platforms that provide practical guidance on cyber security best practices, tools, legal and regulatory requirements, and risk assessment and management for Vietnamese SMEs.
- Adopt a multi-level change model that incorporates change and transformation strategies that encompass initiatives at an individual level (e.g., awareness campaigns), organisational level (e.g. capability development) and governmental level (e.g. policy changes) to facilitate the implementation of effective cyber security measures.

Bibliography

Ahn Duc, "Cisco report on cyberattack threat among Vietnamese SMEs", Vietnam Investment Review, 2021, accessed 22 April 2023, https://vir.com.vn/cisco-report-on-cyberattact-threat-among-vietnamese-smes-88307.html.

AP Hiep Pham, "2022 Vietnam SME Cyber-Fitness", Centre of Cyber security Research and Innovation, 2022.

APEC Small and Medium Enterprises Working Group, "What comes after SME Digital Transformation? – Measuring Effectiveness of Public Policy and Identifying Trends for the Post-Digital Era", 2020, accessed April 25, 2023, https://www.apec.org/docs/default-source/publications/2023/4/what-comes-after-sme-digital-transformation/223_sme_what-comes-after-sme-digital-transfromation.pdf.

AT Kearny, "Cyber security in ASEAN: An urgent call to action", AT Kearny, 2018.

Bharath Aiyer, Venky Anant, and Daniele Di Mattia, "Securing small and medium-size enterprises: What's next?", McKinsey & Company, 2021, accessed April 25, 2023, https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/securing-small-and-medium-size-enterprises-whats-next.

Bkav, "Vietnam cyber security overview in 2022 and predictions for 2023", Bkav Security Solutions, 2022, accessed April 26, 2023, https://www.bkav.com/top-new/-/view-content/1468938/vietnam-cyber-security-overview-in-2022-and-predictions-for-2023.

Cisco, "Cyber security for SMBs: Asia Pacific Businesses Prepare for Digital Defense", Cisco, 2021, accessed April 25, 2023, https://www.cisco.com/c/dam/global/en_sg/products/security/meet-max-report-2021/assets/data/cyber security-for-smbs-asia-pacific-businesses-prepare-for-digital-defense.pdf.

Cisco, "Cisco Cyber security Readiness Index: Resilience in a Hybrid World", Cisco, 2023.

Collett, Robert, and Nayia Barmpaliou, "International Cyber Capacity Building: Global Trends and Scenarios", European Union Institute for Security Studies, 2021, accessed April 25, 2023, https://www.iss.europa.eu/sites/default/files/EUISSFiles/CCB%20Report%20Final.pdf.

Department of Foreign Affairs and Trade (DFAT). "Australia's International Cyber and Critical Tech Engagement." Cyber and Critical Tech Cooperation Program, 2022, accessed April 25, 2023, https://www.internationalcybertech.gov.au/.

Department of Foreign Affairs and Trade, "International Cyber and Critical Tech Engagement Strategy", 2021, accessed 23 April 2023, https://www.internationalcybertech.gov.au/.

Department of Industry, Science, Energy and Resources, "Digital Business Tools," Australian Government, accessed April 25, 2023, https://digitaltools.business.gov.au/.

Dopfer, Kurt, John Foster & Jason Potts, "Micro-Meso-Macro", Journal of Evolutionary Economics, (2004).

Digital McKinsey and Global Risk Practice, "Perspectives on transforming cyber security", McKinsey & Company, 2019.

Francisco Carías, Juan, Saioa Arrizabalaga, Leire Labaka, and Josune Hernantes, "Cyber Resilience Self-Assessment Tool (CR-SAT) for SMEs", IEEE, 2021.

General Statistics Office of Vietnam, "Statistical Yearbook of Vietnam 2021", Vietnam Government, 2022, accessed 20 April 2023, https://www.gso.gov.vn/wp-content/uploads/2022/08/Sach-Nien-giam-TK-2021.pdf.

GoBusiness Singapore & Infocomm Media Development Authority, "CTO-as-a-Service", Infocomm Media, 2023.

Hoang, Ngoc, "Small and medium-sized enterprises approach a cyber-secure future", RMIT, 2022, accessed April 25, 2023, https://www.rmit.edu.vn/news/all-news/2022/jan/small-and-medium-sized-enterprises-approach-a-cyber-secure-future.

Library of Congress, "Vietnam: Support for Small and Medium-Sized Enterprises." Global Legal Monitor, Library of Congress, July 18, 2017, accessed May 15, 2023, https://www.loc.gov/item/global-legal-monitor/2017-07-18/vietnam-support-for-small-and-medium-sized-enterprises.

Mee, Paul, and Rico Brandenburg, "After reading, writing and arithmetic, the 4th 'r' of literacy is cyber-risk", World Economic Forum, 2020, accessed April 25, 2023, https://www.weforum.org/agenda/2020/12/cyber-risk-cyber-security-education.

Ministry of Information and Communications, "Cyber attacks rise in Vietnam", Vietnam Government, 2022, accessed 21 April 2023, https://english.mic.gov.vn.

Ministry of Information and Communications, "National Cyber Security and Safety Strategy: 2025-2030", Vietnam Government, 2022.

Oi, Rebecca, "Cyber security is still challenging for ASEAN businesses", Tech Wire Asia, 2021, Accessed April 25, 2023, https://techwireasia.com/2021/11/cyber security-are-challenging-asean-businesses/.

Raska, Michael and Benjamin Ang, "Cyber security in Southeast Asia", Asia Centre, 2018, accessed April 25, 2023, https://asiacentre.eu/wp-content/uploads/2021/11/NotePresentation-AngRaska-Cyber security_180518.pdf.

RMIT, "Big cyber security questions for small business: The state of cyber fitness in Australian small businesses", RMIT, 2021, accessed 17 May 2023, https://cynch.com.au/small-business-cyber-fitness-2021.

Segal, Edward. "Small Businesses Are More Frequent Targets of Cyberattacks Than Larger Companies: New Report", Forbes, 2022, accessed April 25, 2023. https://www.forbes.com/sites/edwardsegal/2022/03/30/cyber-criminals/?sh=1edc34f352ae.

Shojaifar, Alireza, Samuel A. Fricker, and Martin Gwerder, "Automating the Communication of Cyber security Knowledge: Multi-Case Study", In Information Security Education: Information Security in Action 2020, 109-122. Springer, 2020.

Shojaifar, Alireza, and Heini Järvinen, "Classifying SMEs for Approaching Cyber security Competence and Awareness", 16th International Conference on Availability, Reliability and Security, 2021.

The ASEAN, "Digital Transformation – Issue 23." The ASEAN, 2022, accessed April 25, 2023, https://asean.org/wp-content/uploads/2022/11/Issue-23-Digital-Transformation-digital-version.pdf.

van Haastrecht, Max, Injy Sarhan, Alireza Shojaifar, et al. "A Threat-Based Cyber security Risk Assessment Approach Addressing SME Needs", 16th International Conference on Availability, Reliability and Security, 2021.

Vietnamnet, "Phishing attacks still occurring at the same rate", Vietnamnet, 2022, accessed 22 April, 2023, https://vietnamnet.vn/en/phishing-attacks-still-occurring-at-same-rate-2069989.html.

Vietnam News, "Kaspersky launches new cyber security solution for small and medium sized businesses", Vietnam News (Eng), 2021, accessed 22 April 2023, https://vietnamnews.vn/economy/913131/kaspersky-launches-new-cyber-security-solution-for-small-and-medium-sized-businesses.html.

World Economic Forum, "Global Cyber security Outlook 2022 Insight Report", WEF, 2022, accessed April 25, 2023, https://www3.weforum.org/docs/WEF_Global_Cyber security_Outlook_2022.pdf.

Images

Alexey Godzenko, Blockchain network concept. Distributed ledger technology. Locks are located in Hexagonal cells on black background. 3d rendering illustration. Big data node base concept. Photograph. Shutterstock. Wed 14 June 2023.

Cottonbro Studio/Pexels, Pixabay/Pexels.

Huy Thoai, Da lat, Vietnam - July 8th, 2022: Da Lat city night beautiful tourism destination in central highlands Vietnam. Urban development texture, green parks and lake in Da Lat, Vietnam. Photograph. Shutterstock. Wed 14 June 2023.

JMiks, Login - Username and Password in Internet. Photograph. Shutterstock. Wed 14 June 2023.

Markus Winkler/Unsplash, Philipp Katzenberger/Unsplash, Studio Republic/Unsplash, Tim Gout/Unsplash, Rodion Kutsaiev/Unsplash

Norbert Braun, Blue LEDs in a cube. Photograph. Shutterstock. Wed 14 June 2023.

Acknowledgements

The Australia Vietnam Policy Institute acknowledges the support of the Australian Department of Foreign Affairs and Trade (DFAT).

Creative Commons Licence:

RAPPORTEUR

WRITERS:

The Centre for Cyber Security Research and Innovation (CCSRI), College of Business & Law, RMIT University

Nicola Gibbs

Director, Pluri

RESEARCHERS:

Professor Matt Warren

Director, Centre for Cyber Security Research and Innovation (CCSRI), RMIT University

Associate Professor Pham Cong Hiep

Vietnam Hub Lead, Centre for Cyber Security Research and Innovation (CCSRI), RMIT University

Mr Laki Kondylas

Deputy Director, Centre for Cyber Security Research and Innovation (CCSRI), RMIT University