



[Back](#)

Ethical Thinking in Cyber Resilience: Lessons from Malaysian Cyber Leaders

[Lecture Notes in Networks and Systems](#) • Conference Paper • 2025 •

DOI: 10.1007/978-981-96-6932-5_14

[Molok, Nurul Nuha Abdul](#)^a; [Zulkifli, Zahidah](#)^a ; [Jeong, Jongkil Jay](#)^b; [Maynard, Sean](#)^b; [Ahmad, Atif](#)^b

^aInternational Islamic University Malaysia, Kuala Lumpur, Malaysia

[Show all information](#)

0

Citations

[Full text](#) [Export](#) [Save to list](#)

[Document](#)

[Impact](#)

[Cited by \(0\)](#)

[References \(20\)](#)

[Similar documents](#)

Abstract

This study explores the intersection of ethical thinking and cyber resilience within the context of Malaysian government agencies. Given the increasing reliance on digital infrastructure and the rising threat of cyber-attacks, the need for robust cyber resilience strategies developed by people who are imbued with ethical values, is more critical than ever. However, the role of ethical considerations in shaping these strategies remains underexplored, especially in the public sector. Through a qualitative approach employing interviews as the primary data collection method and thematic analysis as the method for qualitative data analysis, this research proposes the importance of ethics in developing Malaysia's cyber resilience. From the analysis, 4 themes have been identified: moral and spiritual beliefs, alignment to the government agenda, responsibility, and long-term thinking. Findings suggest that ethical thinking plays a crucial role in decision-making processes which influence the development and implementation of cyber-related strategies, policies, and law in Malaysian public sector organisations. This study proposes the integration of ethics in the

development of national cybersecurity strategies, to make the country more resilient to protect itself against cyber threats. © The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2025.

Author keywords

Cyber resilience; Cybersecurity; Ethics; Government; Public sector

Indexed keywords

Engineering controlled terms

Behavioral research; Computer crime; Cybersecurity; Ethical technology; Network security; Public works

Engineering uncontrolled terms

Cybe resilience; Cyber security; Cyber-attacks; Digital infrastructures; Government; Government agencies; Malaysian governments; Malaysians; Public sector; Resilience strategy

Engineering main heading

Decision making

Funding details

Details about financial support for research, including funding sources and grant numbers as provided in academic publications.

Funding sponsor	Funding number	Acronym
International Islamic University		
University of Melbourne See opportunities by UNIMELB		UNIMELB
Department of Foreign Affairs and Trade, Australian Government See opportunities by DFAT		DFAT

Funding text

This study is a part of a collaborative research project between the International Islamic University, Malaysia and the University of Melbourne funded by the Department of Foreign Affairs

and Trade, Australia.

Corresponding authors

Corresponding author

Z. Zulkifli

Affiliation

International Islamic University Malaysia, Kuala Lumpur, Malaysia

Email address

zahidahz@iium.edu.my

© Copyright 2025 Elsevier B.V., All rights reserved.

Abstract

Author keywords

Indexed keywords

Funding details

Corresponding authors

About Scopus

[What is Scopus](#)

[Content coverage](#)

[Scopus blog](#)

[Scopus API](#)

[Privacy matters](#)

Language

[日本語版を表示する](#)

[查看简体中文版本](#)

[查看繁體中文版本](#)

[Просмотр версии на русском языке](#)

Customer Service

[Help](#)

[Tutorials](#)

[Contact us](#)

ELSEVIER

[Terms and conditions](#) ↗ [Privacy policy](#) ↗ [Cookies settings](#)

All content on this site: Copyright © 2026 [Elsevier B.V.](#) ↗, its licensors, and contributors. All rights are reserved, including those for text and data mining, AI training, and similar technologies. For all open access content, the relevant licensing terms apply.

