Enhancing Cybersecurity in Water Sector: Analyzing the Factors Influencing Attitude towards Cybersecurity in Malaysia's Water Industry

Subramaniam Sri Ramalu

Universiti Utara Malaysia, Malaysia

https://doi.org/10.35609/gcbssproceeding.2025.1(72)

ABSTRACT

Cybersecurity threats are a growing concern around the world. Global spending on cybersecurity and losses due to cyber incidents are worrying. Research has found that the weakest element in the cybersecurity chain is the human factor. The use of security technologies fails to address the problem in instances where employees engage in activities that place both themselves and the company at risk. Hence, the role human factors play in cybersecurity is crucial. In Malaysia, little is known about the behavioral aspects of cybersecurity in the water sector, which is known to be vulnerable to cyber-attacks. The present study aims to examine the effects of information security issues awareness, top management support, leadership, information security policy, and cybersecurity awareness training on attitudes toward cybersecurity. The data were collected from 425 respondents from four water companies located in the northern states of Malaysia. The respondents were selected using a disproportionate stratified random sampling technique. The survey was conducted using a questionnaire, and PLS-SEM was used to test the proposed hypotheses. The results show that security issues awareness and top management support are positively related to attitudes toward cybersecurity. However, some hypotheses were not supported. Specifically, the study found that leadership, information security policy, and cybersecurity awareness training did not have a significant positive relationship with attitudes toward cybersecurity. This finding suggests that while these factors may play a role in the broader cybersecurity landscape, they may not directly influence individual attitudes or behaviors as expected. This could be due to various reasons such as the effectiveness of policies, the quality of training, or the lack of consistency in leadership support. The findings have several theoretical and practical implications. By ensuring cybersecurity through compliance behavior, water security is preserved, thus ensuring the well-being of people, as water is a fundamental need for human life. The stability and security of the country can also be maintained with secure and sustainable water resiliency. Finally, economic losses due to cyber-attacks can be reduced.

JEL Codes: L95, O33, D91

Keywords: *Cybersecurity, Water Sector, Risky Cybersecurity Behaviour, Employees.*