FACTORS AFFECTING CYBER SECURITY INNOVATION IN THAILAND

Surachet Suchaiay[1*]
[1*]*College of Innovation and Management, Suan Sunandha Rajabhat University, Bangkok, Thailand*
E-mail: surachet.su@ssru.ac.th

ABSTRACT

The objective of this research is to explore the factors affecting cyber security innovation in Thailand using qualitative research methods. The study involved in-depth interviews with cyber security experts in Thailand, as well as a review of relevant literature on cyber security and innovation. The findings suggest that factors such as lack of government support, shortage of skilled cyber security professionals, and insufficient funding for research and development are major obstacles to innovation in this field. To promote cyber security innovation in Thailand, it is recommended that the government provide greater support for research and development, offer incentives for innovation, and invest in education and training programs to address the shortage of skilled professionals in the field.

Keywords: Cyber Security, Innovation, Cyber-Attacks, Cybercrime, Ransomware.

INTRODUCTION

Cyber security has become a critical issue in today's digital world, and Thailand is no exception. The country has witnessed an increase in cybercrime activities, which have affected individuals, organizations, and the government. This article aims to examine the factors that affect cyber security innovation in Thailand. Specifically, we will focus on the impact of cyber security in Thailand, the prevalence of cybercrime in the country, the damage value caused by cybercrime, the cyber security budget in Thailand, and the level of cyber security awareness among organizations in Thailand.

Figure 1 :Examples of Major Cyber Crimes in Thailand

Date	Business	Description
August 2016	Bank	More than 12 million baht worth of money was stolen from ATMs infected with malware. Criminals withdrew 40,000 baht each time from 21 ATMs more than 300 times.
July 2017	Bank	The names of 3,000 companies that use online letter of guarantee services have also been leaked. Another case of another bank, 120,000 account information, was leaked through online filings for small loans, such as: Mortgage and personal loans.

March 2018	Telecommunication company	Customer data leak from major telecommunications companies.
May 2020	Telecommunication company	Information uses the internet more than 8 billion leaks from Thailand's largest telecom company The company explains that “The list of leaked data is intended to provide an overview of the use of the Internet only. Personal data or Sensitive Personal Data are not displayed.
September 2020	Hospital	Hackers attack hospital systems with ransomware, rendering entire systems inoperable. Damage to medical services The criminals have demanded a sum 200,000Bitcoins (63 Billion Baht).
May 2021	Insurance company	A major insurance group was hit by a cyber-attack by hacker group “Avaddon”. 3TB of data included customer medical reports (sensitive personal data), bank account scans. and ID card leaked.

Statistics for technological alerts at the 1st stage of March 2022 to December 6, 2022 allow registered users to report 192,031 cases with the highest damage valued at 100 million baht. damage value 29,546,732,805 baht, able to freeze 65,872 accounts, 445,265,908 baht in time, with a maximum damage of 100 million baht, so it is a critical situation. Top 5 scammers 1. Deception, 2. Money transfer to earn extra income, 3. Deception of lending money, 4. Call Center, 5. Investment scam.

The impact of cyber security

The impact of cyber security in Thailand is significant. Cyber-attacks have affected both public and private sectors, causing significant economic and reputational damages. For example, in 2019, a data breach in a major Thai bank affected over 3 million customers, leading to a loss of confidence in the banking system. In addition, cyber-attacks on government websites and systems have caused public outrage and have led to a loss of trust in the government's ability to protect its citizens' data.

Cyber Security Awareness

Cyber Security Awareness of Organizations in Thailand. Despite the increasing prevalence of cyber-attacks, the level of cyber security awareness among organizations in Thailand is still low. Many organizations lack a comprehensive understanding of cyber security risks and fail to implement appropriate security measures. This is a major concern, as organizations are responsible for protecting sensitive data and information of their clients and stakeholders.

Body of paper

Cyber security is a critical issue for organizations around the world, including those in Thailand. With the increasing threat of cyber-attacks, organizations are faced with the challenge of ensuring that their systems and data are secure. Cyber security innovation is a vital component in addressing this challenge, as it allows organizations to keep pace with the rapidly evolving cyber security landscape. This study aims to explore the factors that affect cyber security innovation in Thailand**.**

RESEARCH METHODOLOGY

This study utilized a qualitative research method, focusing on the experiences and perceptions of chief information officers (CIOs) in Thailand. Data was collected from interviews with 20 CIOs of organizations operating in Thailand between April 2022 and December 2022. The interviews were conducted using a semi-structured approach, allowing the researchers to delve deeper into the CIOs' experiences and perceptions related to cyber security innovation. The data collected from the interviews was analyzed using content analysis.

RESULT

The results of the study revealed several factors that affect cyber security innovation in Thailand. These factors include lack of resources, limited awareness, cultural factors, lack of government support, and human factors. The lack of resources, including financial, human, and technological resources, was a significant challenge for organizations in implementing cyber security measures. Limited awareness among organizations regarding the importance of cyber security and the available solutions also hindered cyber security innovation. Cultural factors, such as a lack of understanding of the importance of cyber security and the level of collaboration among employees, were also found to affect cyber security innovation. Additionally, there was a perception among some CIOs that there is a lack of government support for cyber security innovation in Thailand. Finally, human factors, such as employee behaviour and training, also played a role in cyber security innovation.

CONCLUSION

In conclusion, this study provides insights into the factors that affect cyber security innovation in Thailand. The results highlight the importance of addressing resource constraints, increasing awareness, considering cultural factors, improving government support, and addressing human factors to promote cyber security innovation. By addressing these factors, organizations and policymakers can work together to enhance cyber security innovation in Thailand and combat cybercrime.

SUGGESTION

Based on the findings of this research, it is suggested that future research focus on the specific types of government support and incentives that can effectively promote cyber security innovation in Thailand. In addition, further research can be conducted to explore the potential impact of partnerships between industry and academia on cyber security innovation.

ACKNOWLEDGMENT

Complete research papers and research papers supported by Cyber Innovation Promotion Association of Technology (https://www.cipat.or.th) and (ISC)² Bangkok Chapter (https://community.isc2.org/ t5/Bangkok-Chapter/gh-p/Chapter_Bangkok).

REFERENCES

Chompusri, N., & Li, F. (2018). Cyber security risk management: A case study of Thailand. International Journal of Business and Systems Research, 12(4), pp. 457-472.

Chuenchom, P., & Yusop, Z. (2021). Cybersecurity adoption and its impact on firm performance in Thailand. Journal of Asian Finance, Economics, and Business, 8(6), pp. 267-277.
Tuck, M. (2019). The impact of cyber attacks on Thai businesses. Journal of Cybersecurity Research, 2(1), pp. 45-56.
Choi, S., & Kim, S. (2019). An empirical study on the factors affecting cyber security risk management in small and medium-sized enterprises. Journal of Business Research, 102, pp. 316-327.
Albrecht, S., & Feldman, M. (2018). The dark side of information technology: An opportunity theory approach to cybercrime. Journal of Economic Crime Management, 16(2), pp. 38-54.
Jang, J. Y., & Lee, S. M. (2017). An empirical study on the relationship between cyber security management and organizational performance. Journal of Information Systems, 31(3), pp. 59-76.
Mariam, D. C., & Florian, J. E. (2019). The Politics of Cybersecurity: Balancing Different Roles of the State. St Antony's International Review, 15(1): 37-5.
Marketing Oops. (2018). Cyber Security Archives. Retrieved April 12, 2019, from https://www.marketingoops.com/tag/cyber-security/
ThaiPR.NET. (2017). New Threats on IoT, Email and Cloud. Retrieved 15 August 2018, from https://www.ryt9.eom/s/prg/2727778