Asia Pacific, 2024
Vol. 42, pp. 97 – 111

SOUTHEAST ASIA AND GROWING CHALLENGE OF CYBER-ATTACKS: A REGIONAL SECURITY INSIGHT

*Jawad Hussain Awan**
Syed Raza Hussain Shah†
Khalid Charan‡

ABSTRACT

Southeast Asia is the one of fastest-rising internet marketplace internationally, with its digital economy predictable to extent a gross merchandise worth of more than $500 billion by 2030. However, this fast digital growth has also activated an important growth in cybercrime, which augmented by 85 per cent from 2020 to 2024. This upwelling emphasizes the serious necessity to identify cyber-attacks, mainly directing the under banked population, who are particularly at threat due to least digital knowledge and their dependence on familiar business services. In user surveys, most of the respondents reported cyber-targets weekly across Southeast Asian countries (i.e. Indonesia Taiwan, Malaysia, Korea, the Philippines, Singapore, Hong Kong, and Thailand). The amount totalling of 225 million in 2023, are mainly unprotected to cyber risks due to partial digital knowledge and reliance on uncertain monetary services with lowest entry hurdles. This paper finds that establishing cyber security, improving monetary knowledge, and nurturing regional partnership are important stages to safeguard these susceptible groups from the rising cyber threat to the nations of the region.

Keywords: *Cyber-crime, internet, digital economy and Southeast Asia*

*Faculty of Engineering, Sciences and Technology, Iqra University, Karachi Email: jawad.hussain@iqra.edu.pk (Corresponding Author)
†Faculty of Engineering and Technology, University of Sindh, Jamshoro Email: raza.shah@usindh.edu.pk
‡Faculty of Engineering, Science and Technology, Hamdard University, Karachi Email:khalid.charan@hamdard.edu.pk

INTRODUCTION

ASEAN has prepared significant progress in forming a framework for integrated methods to cyber-threats (ASEAN Cybersecurity Cooperation, 2023). However, surplus work is mandatory before regional engagements are vigorous enough to provide shared support during national cyber disasters. This necessity for restructuring is flattering more persistent due to the cyber-risks modelled to regional critical data structure by fast digitalisation, rising cyber-crime, and deteriorating geopolitical pressures. As per the ASEAN annual report (ASEAN, 2023), ASEAN can improve joint-response approaches through deeper political, practical, and operational synchronisation. The EU and the US established prototypes as a depiction on cyber-emergency response (EU Cybersecurity Agency, 2023).

The rate of cyber-crimes in Southeast Asia has increased in capacity and density since the last decade, determined by aspects such as the deluge in connectivity during the COVID-19 pandemic, the broader usage of AI and other advanced technologies, and the region's rising eminence as an objective for cyber reconnaissance due to its growing geopolitical significance (Asia-Pacific Cybersecurity Association, 2023). The reviews for the present existence of cybersecurity cooperation among ASEAN countries were carried out and then discussed the responses received from the regional level of cyber emergencies within the Southeast Asian perspective. From the response of cyber-emergency prototypes in the EU and the US, the study finds research gaps in ASEAN's cybersecurity cooperation context and proposes serious regions for growth in forming a regional cyber-emergency arrangement. The outcomes also support ASEAN's durable objective of applying UN-endorsed standards for shared support in the occurrence of a cyber-attack (United Nations Cybersecurity Task Force, 2023).

The efforts initiated in the early 2000s enhanced the regional ICT sectors and also the cooperation of ASEAN member states has become strong in developing Computer Emergency Response Teams

(CERTs) (ASEAN ICT Strategy, 2022). However, ASEAN has motivated reinforcing CERT cooperation. Whereas the challenges and issues reported in cybersecurity were discussed in economic or political platforms, now there is a separate platform to discuss cybersecurity-related issues. The protection of Critical Infrastructures has also been emphasized during cyber emergency meetings and discussions. Additionally, various initiatives linking dialogue partners, global sectors, and private organizations have been taken to improve the cybersecurity of the region and nurture better shared trust among the member states of ASEAN (Cybersecurity Development Group, 2023).

Malaysia and Singapore are active in primary multi-shareholder struggles and launching data sharing approaches in internal sectors, i.e., defense (Southeast Asia Cyber Defense Cooperation, 2023). Notwithstanding growth in data sharing and capacity building to boost readiness for cyber-attacks on Critical Infrastructure (National Cyber Security Centre, 2023), ASEAN's patchy cybersecurity design still delays additional progress. Member states of ASEAN have diverse phases of cybersecurity development, and the region lacks an integrated cyber dictionary, adequate cybersecurity specialists, and a deliberate method to cybersecurity. The study also outlines important phases to producing an ASEAN cyber-emergency response context, endorsing the identification of priority critical infrastructure regions in separate member states and stronger regional sustenance for UN-endorsed cyber standards. During the interconnected globe, the timely establishment of a cyber-emergency-response context for ASEAN states plays an important role in strengthening the resilience systems of the region and provides a flexible environment to other states with least capacity and management of growing cybercrimes (Cyber Resilience Coalition, 2023).

LITERATURE REVIEW

From the studies (Cyber security Research Institute. 2023) (Global Cybersecurity Council, 2023), the global distribution of cyber-attacks

is illustrated in Figure 01. From the illustration, it is noticed that Europe is the leading with 13.3%, Southeast Asia on second with 12.9%, Japan on third with 12.5%, USA on fourth with 10.8%, India on fifth with 7.1%, UK on sixth with 6.4%, Germany on seventh with 5.4%, South Korea on eighth with 5. 2%, Australia on ninth with 4.8%, Non-EU states of Europe on tenth with 4.4%, France on eleventh with 4.1%, Canada on twelfth with 2.9%, and East Asia on thirteenth with 2.3%, and others have 7.7% share in reporting of cyber-attacks. Southeast Asia became a central point for reconnaissance actions, linking the gap between NATO and other nations like North Korea, Russia, Iran, and China.

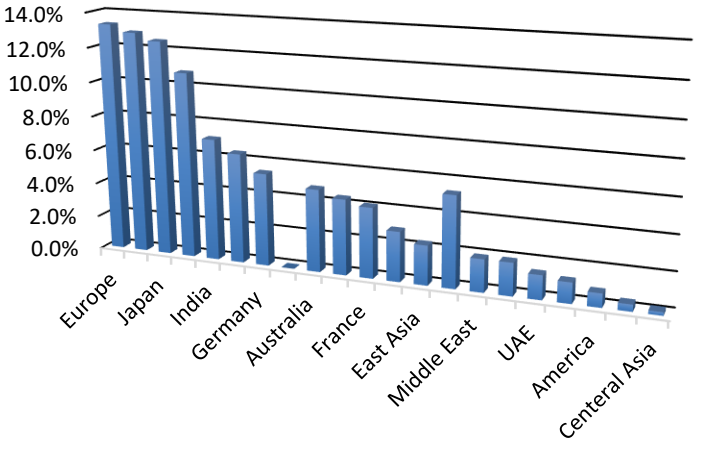

Figure 01: Anti-Scam Report of the Global Anti-Scam Alliance

The details of the cyber-attacks reported in Southeast Asia from 2023 to 2024, discussing the Country (including Thailand, Singapore, Vietnam, Indonesia, the Philippines, Singapore and Malaysia), description of cyber-attack, Impact and Analysis of reported cyber-attack are giving in the following table.

Table I: Reported Notable cyber-attacks in Southeast Asia from 2023 to 2024

References	Country	Description of cyber-attack	Impact	Analysis
NCSA Thailand, Cybersecurity reports (NCSA, 2023)	Thailand	The government websites were targeted using APT38 and these were state-sponsored, distracting the operations of public organizations and data theft of sensitive government information.	This cyber-attack resulted distracting the public services and leaked the information of government institutes.	This happened due to politically motivation, and intended at information theft and disrupting the operations of government services.
Ministry of Health Singapore, Sing Health Reports (MoHS, 2018)	Singapore	In this cyber-attack, huge number of medical health records of patients have been exposed including Prime Minister of the state. The attack was targeted on Sing Health.	More than 1.5 million records of patients compromised.	The data breach identified various weaknesses in healthcare systems and the essential for improved data security.
Ministry of Information and Communications Vietnam (MICV, 2020)	Vietnam	This cyber-attack breach has targeted South China Sea-related information And known as "State-sponsored".	The military, economic and political data was compromised.	This was named as "Cyber espionage", aiming to disrupt Vietnam's strategic and political interests.
Kominfo Indonesia, Cybersecurity audits (Kominfo, 2022)	Indonesia	This cyber-attack targeted mobile applications, cellphones and government platform applications, which affected nearly 7 million users.	This data theft attack exposed sensitive information i-e: personal and financial data.	This mechanism highlighted vulnerabilities, weak data protection approaches used in digital services.

COMELEC Philippines, International Election Security (COMELEC, 2022)	Philippines	This cyber-attack was the DDoS, aimed to disrupt election infrastructure of Philippines during arrangements for local elections.	Online election system's service was disrupted and possible cyber-risk.	Identified weakness in electoral systems, levitation alarms the integrity of Philippines election ruled in Southeast Asia.
MAS Singapore, Trend Micro, Cybersecurity reports (MAS, 2021)	Singapore	This cyber-attack targeted key banks, interconnected to APT groups, intended to data theft and financial espionage.	This attack disrupted the banking information by compromising financial services.	This cyber-attack steal the sensitive information of banking customers and compromised the operations for malicious purpose.
Cybersecurity Malaysia, Ransomware threat reports (CySec Malaysia, 2023)	Malaysia	This ransomware attack targeted various government corporations, requiring cryptocurrency.	Financial and operational losses reported by disrupting corporation's services.	This ransomware identified The growing rate of vulnerabilities carried out in businesses of Southeast Asian states.

These cyber-attacks reported across Southeast Asian states in 2023 and 2024 emphasise the rising and developing cybersecurity cyber-threats confronted by the Southeast Asian region summarised in above Table I. these cyber-attacks disrupted the critical services or government system's operations, although, there were also intended to use in economic, political, and social affects. Additionally, it is critical for the business sectors, government institutes, and regional organisations to improve cooperation, reinforce cybersecurity infrastructure, and apply additional vigorous data protection processes to alleviate imminent cyber-threats and certify flexibility in the growing usage of digital world.

Phishing Attacks Across Industries

CYFIRMA (2024), cyber-threat Landscape Corporation published a report about the industries, in which the statistics of cutting-edge cyber security and their understandings on worldwide industries discussed. In following figure 02, the recorded phishing attacks are

illustrated and the data has been derived from origin report of ASN. From the research, it is identified that Southeast Asian countries are attractive locations for malicious activities i-e: Singapore, Vietnam, Indonesia, and Malaysia. VPSs and VPNs are most attentive targets for these states as deprived from the research reports.

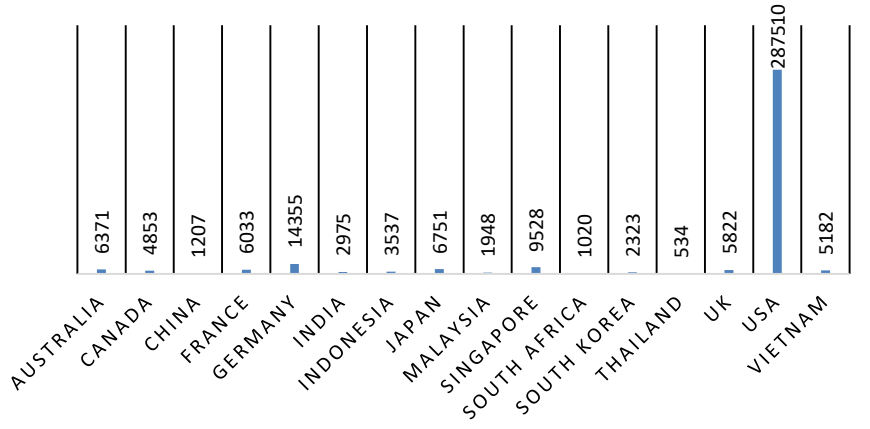

Figure 02: Globally recorded cases of Phishing

FINDINGS, DISCUSSION AND ANALYSIS

Cybersecurity Vulnerabilities in Southeast Asia's Digital Growth

Southeast Asian countries are playing an important role in the digital market, and Indonesia is one of the major states of Southeast Asia, whose transaction value was $77 billion in 2022 (ASEAN Digital Market Report, 2023), accounting for 40% of the total market value. Indonesia continues to play a fundamental part in the region's digital economic matters. In this way, the investment is expected to double or triple by 2025, which will make Indonesia a stronger contributor (Indonesia Digital Economic Outlook, 2023). Singapore and Malaysia have also contributed to making Southeast Asia one of the top regions globally with more than 2,400 start-ups (Southeast Asia Innovation Report, 2023).

As part of its ASEAN agenda, the states are dedicated to driving the digital revolution in the imminent years. However, this fast digital

progress also exposes ASEAN to major challenges, particularly in the realm of cybersecurity. The states face cyber risks related to data breaches from various government agencies, enterprises, and financial services, potentially affecting many entities. Information disclosures and identity theft are the most commonly cited issues. The Ministry of Communications and Informatics (MoCI) in 2021 reported that more than 90% of data breaches were attributed to fundamental cybersecurity weaknesses (Ministry of Communications and Informatics [MoCI], 2021). This highlights the crucial need for ASEAN to enhance its efforts in building a cyber-resilience environment.

Rising Cyber Threats & Lack of Awareness in Southeast Asia

Cyber-resilience in Southeast Asia remains a critical concern due to suspicions surrounding the region's awareness of the digital revolution spreading across various industries. In 2022, Indonesia's National Cyber and Crypto Agency (BSSN) reported that more than 10 million cyber-attack cases were recorded, including malware (nearly 50%), data leaks (15%), Trojan attacks (10%), and others (BSSN, 2022). The year 2023 was particularly alarming, with over 347 million cyber-attacks reported, with ransomware emerging as the most dominant threat (Cyber security Agency, 2023). The lack of consistent cyber security principles and guidelines across ASEAN is a leading issue, resulting in fragmented defense systems and weaknesses in cross-border collaboration (ASEAN Cybersecurity Cooperation, 2023). Furthermore, the region's shortage of skilled cyber security professionals and irregular delivery of cyber security resources have delayed efforts to establish robust systems. Several Southeast Asian countries also face a lack of public awareness about cyber-threats, making individuals and organizations more vulnerable to social engineering attacks such as ransomware (Southeast Asia Cyber Defense Report, 2023). Another significant challenge is the rapidly evolving nature of cyber-threats, which outpace existing defense capabilities, demanding constant adaptation and innovation. Addressing these challenges requires nurturing durable partnerships

between governments, private organizations, and the international sector, creating comprehensive cyber security frameworks, promoting cyber education, and advancing cutting-edge technologies like AI for cyber-threat detection (Cyber Resilience Coalition, 2023). By implementing these measures, Southeast Asia can build a more robust cyber security environment to protect its growing digital economy.

Anti-Scam Report on Global Anti-Scam Alliance

The recent Anti-Scam Report (Global Anti-Scam Alliance & Gogolook, 2023) is published in 2023, the report highlighted the growing surge of virtual scams and online fraudulent happenings those have been progressively effecting worldwide digital societies. It identifies the practice of strategies such as identity theft, phishing, and forged investment, which have become further deceiving and firmer to discover. Moreover, the report emphasizes the significant economic losses acquired by victims, noting that several entities and industries are dropping victim to scams due to nonexistence of responsiveness, cyber security awareness, and confidence in digital communications. The figure 03 illustrates the cyber-attacks reported every day, weekly, once a week, monthly, every month, and never for the ASEAN countries including Taiwan, Thailand, Japan, Korea, the Philippines, Malaysia, Hong Kong, Singapore, Vietnam, China, and Indonesia.

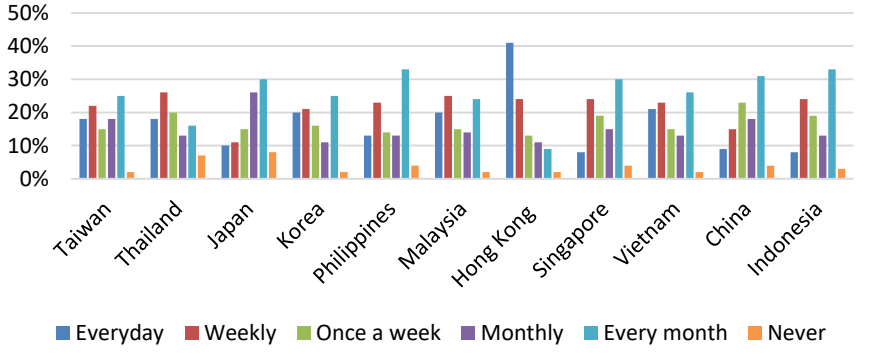

Figure 03: Anti-Scam Report by the Global Anti-Scam Alliance (Global Anti-Scam Alliance & Gogolook, 2023)

The response from the GASA promotes the improved public learning, enhanced discovery tools, and solider corporations between managements, private corporations, and clients to alleviate the effect of scams and increase global digital safety.

Ransomware Groups and their Role in Cybersecurity Losses

From the following figure 04, it can be acknowledged that ransomeware cyber-attacks had a slow beginning. Initially, the government cyber security approaches played crucial role, unfortunately, FIN11, Conti and TA505 criminal groups regrouped in 2023 and formed as a ransomeware named as Clop, which is largest malicious ransomeware and MoveIt became older one after the launch of Clop. Further illustration is shown in figure 04 for the ransomeware activities recorded from January 2023 to July 2023 (Smith, J., & Adams, R., 2023) (Trend Micro, 2023) (Kaspersky, 2023) (Symantec Corporation, 2023). The following illustration highlights the control of key ransomware cyber-criminal activists. Concurrently, it can be notified that the shared action of smaller criminal groups contributes to a considerable ratio of losses.

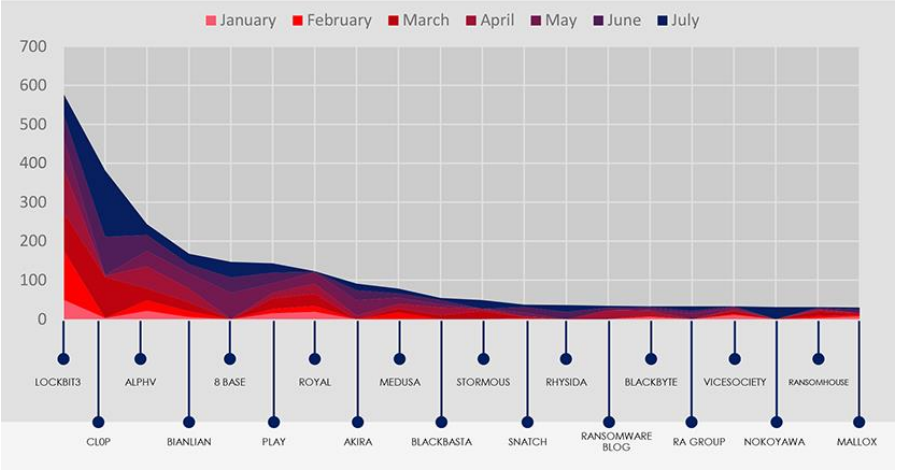

Figure 04: Globally recorded cases of Phishing (CYFIRMA, 2024)

RANSOMWARE LANDSCAPE IN SOUTHEAST ASIA

From the studies (Europol, 2023), it is noticed that 54 ransomeware cybercriminal groups have been recorded and sixteen of them are actively working in the Southeast Asian states. LockBit3 is the most active gang claiming 47% criminal activities as shown in following figure 05. Alphvm is on second and Clop on third while Snatch is a least active criminal group in Southeast Asia.

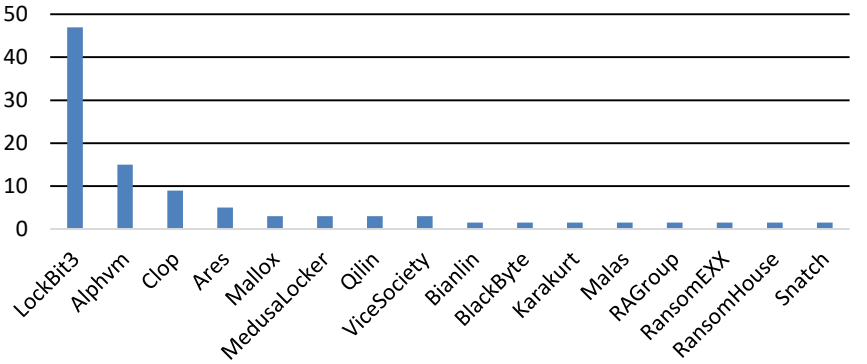

Figure 05: Globally recorded cases of Phishing

CYBER SECURITY STRATEGIES FOR SOUTHEAST ASIA: SAFEGUARDING CRITICAL INFRASTRUCTURE AND TRADE

Southeast Asian state government need to adopt various defensive processes to hostage the rising cyber-threat in their digital cyberspace. An initial and strategic stage is to emphasis on capacity-building trainings across Southeast Asian member states, mainly enhancing critical infrastructure and evolving skilled-personal to warfare cyber intrusions. The region could benefit from Australian Signals Directorate, it conducts vital research on the advancements of information security utilizing schools, colleges and university students, and offering an enduring solution to the growing cyber-threat. Moreover, launching a cyber-security economic region that observes to global cybersecurity principles, which is crucial for defending the supply chain, from strategy to distribution, whereas safeguarding the safety of online transactions. This approach would

strengthen regional trade safety and provide comprehensive constancy in the aspect of growing cybercrime action. The mitigation process against cyber targets reported in the region are also in its early phases, and the governments must apply and implement data disclosure and breaches cyber-laws efficiently. Meanwhile, the organizations require to update and adopt cybersecurity approaches. These approaches could support decrease the rising modelled cyber-risks internationally.

CONCLUSION

Southeast Asia is known as "Regional Hub", aiming to support regional cyber security competences, support to comprehensive cyber security struggles, and endorse a secure and safe digital context in Southeast Asia. Southeast Asia became the attention of state-sponsored, mainly interconnected to North Korea, Vietnam, and China. While, Singapore is a strategic state situated as an unbiased diplomatic hub in the region, has developed into a key focus for reconnaissance, including in cyberspace, interesting states globally. Phishing remains a rising alarm, with a concerning tendency of small to mid-skilled criminals unstable from traditional crimes to cyber-crime. This change aligns with the region's enhanced digital growth and development. The origins of Autonomous System Number placed Singapore as fifth state in phishing campaign and prosperous industrial sector of Southeast Asian countries makes it a primary target of ransomware cyber-attacks. Additionally, 1/10 ransomware cyber-attack is reported from prosperous industrial sector, and Lockbit3 ransomware group is highly active group of the region. Besides, Singapore is now world's most famous state and may be a future target of modern cyber activists, state-sponsored groups, and cyber-threat actors. By enhancing the cooperation, exchange of knowledge, partnerships, capacity building activities and awareness campaigns may develop sustainable platforms to enhance cyber capabilities and highlights the issues and challenges dealt by regional Southeast Asian states.

REFERENCES

ASEAN (2023). *ASEAN annual report: Cybersecurity cooperation and progress*.

ASEAN Cyber Security Cooperation. (2023). *Cyber security frameworks and regional responses*. https://www.asean-cybersecurity.org

ASEAN Cybersecurity Cooperation. (2023). Cybersecurity frameworks and regional collaboration in Southeast Asia.

ASEAN Digital Market Report. (2023). *Southeast Asia's digital economy: The growth and future prospects*. ASEAN Economic Cooperation.

ASEAN ICT Strategy. (2022). *ICT sector development and cybersecurity progress in ASEAN*.

Asia-Pacific Cybersecurity Association. (2023). *Cyber-crime trends in Southeast Asia and their geopolitical implications*.

BSSN (National Cyber and Crypto Agency). (2022). Annual cyber-attack report: Trends and statistics.

Commission on Elections (COMELEC) Philippines. (2022). *International election security: Cyber threats on election infrastructure*.

Cybersecurity Agency. (2023). Cyber-attack statistics and threats in Southeast Asia.

Cyber Resilience Coalition. (2023). *Strengthening regional cyber resilience: ASEAN's role in a connected world*.

Cyber Resilience Coalition. (2023). Building resilience in Southeast Asia's digital economy. https://www.cyberresiliencecoalition.org

Cyber security Development Group. (2023). *Cyber security in ASEAN: Building trust through international partnerships*.

Cybersecurity Malaysia. (2023). *Ransomware threat reports: Attacks on government corporations*. Cybersecurity Malaysia.

Cybersecurity Research Institute. (2023). *Global distribution of cyber-attacks: Trends and analysis*. Cybersecurity Research Institute.

CYFIRMA. (2024). *Cyber-threat landscape: Global industries and phishing attacks*. Cyber-threat Landscape Corporation.

EU Cyber security Agency. (2023). *Cyber-emergency response models: Lessons from the EU and the US*.

Europol. (2023). *Ransomware in Southeast Asia: A threat analysis*. Europol.

Global Anti-Scam Alliance & Gogolook. (2023). *Anti-Scam Report 2023: The rise of online frauds and virtual scams*.

Global Cybersecurity Council. (2023). *Cyber-attacks in Southeast Asia: Trends and national security risks*. Global Cybersecurity Council.

Indonesia Digital Economic Outlook. (2023). Indonesia's growing role in the digital economy. Indonesia Ministry of Digital Economy.

Kaspersky Labs. (2023). *The rise of ransomware: Insights into cybercriminal groups and their operations*. Kaspersky.

Kominfo Indonesia. (2022). *Cybersecurity audits and mobile application vulnerabilities*. Ministry of Communications and Information Technology, Indonesia.

Ministry of Health Singapore. (2018). *SingHealth cyber-attack report: Breach of medical records*. Ministry of Health Singapore.

Ministry of Information and Communications Vietnam. (2020). *Cybersecurity threat reports: Targeting South China Sea-related information*. Ministry of Information and Communications Vietnam.

Ministry of Communications and Informatics [MoCI]. (2021). Annual report on *cybersecurity and data breaches in Indonesia*. https://www.moci.go.idNational Cyber Security Centre. (2023). *Building ASEAN's capacity for critical infrastructure protection*.

Monetary Authority of Singapore (MAS). (2021). *Cybersecurity reports on banking sector vulnerabilities and financial espionage*.

National Cyber Security Agency Thailand. (2023). *Cybersecurity reports on targeted government websites and data theft*. National Cyber Security Agency Thailand.

Smith, J., & Adams, R. (2023). Ransomware: A growing threat to global cybersecurity. *Journal of Cybersecurity Research*, 15(3), 142-157. https://doi.org/10.1016/j.jcsr.2023.01.003

Southeast Asia Cyber Defense Cooperation. (2023). *Data-sharing approaches in defense and cybersecurity*.

Southeast Asia Cyber Defense Report. (2023). The evolving cyber-threat landscape and national responses in Southeast Asia.

Southeast Asia Innovation Report. (2023). Startups and innovation in Southeast Asia: A report on the growth of tech industries. Southeast Asia Development Group.

Symantec Corporation. (2023). *The role of ransomware gangs in cybersecurity incidents*. Symantec Threat Intelligence Report.

Trend Micro. (2023). *Ransomware in Southeast Asia: An analysis of the growing threat*. Trend Micro. Retrieved from https://www.trendmicro.com/southeast-asia-ransomware-report (accessed: Oct. 25, 2024)

United Nations Cybersecurity Task Force. (2023). *Global standards for cybersecurity and shared support frameworks*.

Received: Nov. 5, 2024
Revision Received: Dec. 25, 2024
Published: Dec. 31, 2024