International Conference on Social Science and Humanity
Homepage : https://proceeding.antispublisher.or.id/index.php/icossh
Email : admin@antispublisher.com

e-ISSN : 3063-9611
ICOSSH, Vol. 2, No. 2, 2025
Page 81-94

Cyber Security in Thailand: A Mission Towards Safety in the Digital Age

Thipphawan Poonsawat
Burapha University, Thailand

DOI : https://doi.org/10.61796/icossh.v2i2.21

Sections Info

Article history:
Submitted: February 10, 2025
Final Revised: March 28, 2025
Accepted: April 14, 2025
Published: May 24, 2025

Keywords:
Cybersecurity
Policy
Law
Digital age
Cooperation

ABSTRACT

Objective: *This article aims to examine the development and implementation of cybersecurity measures in Thailand, focusing on the creation of cybersecurity frameworks, national policies, and strategic guidelines.* ***Method:*** *The study employs a qualitative descriptive approach using secondary data from government documents, legal frameworks, and cybersecurity policy analyses.* ***Results:*** *The findings reveal that Thailand has taken significant steps toward enhancing cybersecurity through legislative measures on personal data protection, public awareness campaigns on cyber threats, and the establishment of specialized cybersecurity agencies. Moreover, Thailand has collaborated with international partners to strengthen its cybersecurity infrastructure, thereby fostering public and institutional trust in digital services and enhancing national security.* ***Novelty:*** *This study contributes a comprehensive overview of Thailand's cybersecurity evolution, emphasizing not only the importance of legal and institutional mechanisms but also the strategic role of public engagement and international cooperation. The article offers practical guidelines for further strengthening cybersecurity systems in Thailand to align with global standards and addresses key challenges in achieving robust digital security across sectors.*

INTRODUCTION

Currently, Thailand has entered the digital age. This is an era in which digital technology has played a role in everyone's daily life. in terms of economy, society and security. Various organizations, whether government agencies or the private sector, have used various digital technologies in their organizations [1]. Various formats In order to keep up with technology And there is also a system for linking information access. between government agencies private sector agencies and citizens to increase convenience and speed for those who want to contact that organization [2]. Most of the information will be stored, processed, and forwarded in digital form. Thailand to provide physical treatment for the benefit of maintaining security and safety of the people from nutritional threats in various forms [3].

RESEARCH METHOD

This article is a qualitative research method. The researcher studied information sources from textbooks, literature reviews, articles, research documents and various websites. The research results are used to propose guidelines for creating cyber security in Thailand.

Literature review

Cyber security

From the study, it was found that Chatuchak Paengchan defined cyber security as a process that will make the organization free from risks and dangers that affect the

security of information in all forms, both electronic and physical, including the security of information systems and networks used to store, access, process and distribute that information. It also includes prevention against crimes, attacks, sabotage, espionage, accidents and errors of the organization's information. And the International Telecommunication Union (ITU) has defined the term "cyber security" as "a collection of policy tools, security concepts, security concepts, guidelines, risk management methods, operations, training, good practices and technologies that can be used to protect cyber environment, including the assets of the organization and users, which includes computer equipment, infrastructure, applications, services, communication systems, including all information that is transferred and or stored in the cyber environment. In summary, Cyber Security is the need to protect and maintain the security of computer systems, network systems and related information. The purpose is to prevent access, modification, alteration or destruction of information from unauthorized persons or persons who want to access information for improper purposes [4].

Building cyber security

From the study of cybersecurity, Methaporn Thammasiri and Siriphat Wongthongdee stated that cybersecurity means any method, measure or action to prevent, cope with, mitigate and reduce the risk from cyber threats that affect the factors of confidentiality, integrity and availability of devices and data in the information system. If cybersecurity is weak, it may allow malicious individuals to damage the user and their personal data. Meanwhile, the Defense Technology Analysis Division of the Defense Technology Institute stated that cybersecurity is creating security in the network and data system. To achieve this objective, both technological measures, legal measures, self-regulation and joint supervision of all three parties affected by cyber attacks are required: the state, private sector and the public. In summary, cybersecurity is a method, measure or action taken to prevent and prepare for cyber threats, which all parties involved must jointly implement, whether the state, private sector or the public [5].

Building cyber security in Thailand

From the study on the creation of cybersecurity in Thailand by Charinthip Pansuwan and the Digital Government Development Agency (Public Organization), it was found that Thailand places importance on maintaining and creating cybersecurity by implementing several measures as follows:

1. Policy and law formulation
2. Cybersecurity infrastructure development
3. Strengthening international cooperation
4. Raising awareness and developing personnel
5. Research and development of technology
6. Preventing and responding to threats.

Creating cybersecurity in Thailand is a collaboration between many sectors, including the government, private sector, and international organizations. There are policies, laws, and development of necessary infrastructure to prevent cyber threats that may affect national security, economy, and society. In addition, there is an emphasis on

raising awareness and training to increase knowledge and understanding of cybersecurity in all sectors [6].

Thailand's cyber security policy

Cybersecurity policy and action plan (2022-2027)

Strategy 1: Prevent and reduce risks from cyber threats

a. Create security in critical infrastructure such as banking, communications, and energy.
b. Support the development of cybersecurity standards in all sectors.

Strategy 2: Strengthen the capacity to detect and respond to cyber threats.

a. Use AI technology and data analytics to detect threats.
b. Establish a Cyber Security Operation Center (CSOC)

Strategy 3: Develop personnel and raise awareness

a. Increase the number of cybersecurity experts.
b. Organize training and awareness-raising activities for agencies and the public.

Strategy 4: Promote international cooperation

a. Participate in international cooperation forums such as the ASEAN Cybersecurity Cooperation.
b. Exchange threat information with regional partners.

Strategy 5: Create a cybersecurity ecosystem

a. Support research and development of cybersecurity technologies.
b. Develop modern laws and policies to support future threats.

Relevant agencies and their roles in creating cyber security in Thailand

Cybersecurity in Thailand involves many agencies working together in both the public and private sectors to cope with rapidly evolving cyber threats. Each agency has a clear role in preventing, controlling, and responding to cyber incidents to ensure that the use of information technology in the country is safe and does not pose a threat to national security and the economy [7].

Agencies related to Cybersecurity and their roles

1. Electronic Transactions Development Agency (ETDA)

Role: ETDA is a government agency responsible for overseeing electronic transactions (E-Commerce) and personal data protection, as well as promoting the safe use of digital technology.

Duties:

a. Set security standards in the business sector
b. Develop cyber security standards and guidelines
c. Provide training and create understanding of cybersecurity in the business sector
d. Support the use of safe digital services
e. Manage personal data used in electronic transactions

2. National Cyber Security Response Team (ThaiCERT)

Role: ThaiCERT is a key agency responsible for detecting, alerting, to cyber threats, and coordinating with other agencies to respond to national cyber incidents.

Duties:

a. Provide information on cyber threats and prevention methods
b. Respond to cyber incidents such as DDoS attacks, Ransomware, and hacking
c. Provide advice on prevention and management of cyber risks
d. Manage database of cyber- attacks and threats
e. Organize training and enhancing knowledge on cybersecurity

3. Ministry of Digital Economy and Society (MDES)

Role: The Ministry of Digital Economy and Society is the main agency that sets the direction and policy on cybersecurity of the country.

Duties:

a. Set a national cybersecurity policy
b. Integrate cooperation among various government agencies
c. Promote the use of safe digital technology
d. Develop laws and legal frameworks related to cybersecurity
e. Focus on personal data protection and cyber risk management

4. Office of Insurance Commission (OIC)

Role: The OIC oversees insurance and data protection of insured persons, including promoting data system security within the insurance industry

Duties:

a. Set cybersecurity measures and standards for organizations in the insurance industry
b. Supporting customer data protection in cyber systems
c. Prevent misuse of customer data through personal data protection

5. Office of the Auditor General (SAO)

Role: The SAO is an agency that inspects the use of government resources, including the use of information technology in government agencies, to ensure that there is no corruption or misuse of data.

Duties: Inspect the cybersecurity system in government agencies Inspect the use of government data to ensure that it is safe and transparent Provide advice on enhancing data security in government agencies.

Building cyber security in Thailand

The study found that the creation of cybersecurity in Thailand has been carried out in many dimensions, as follows:

1. Legal framework: The law that Thailand has issued to regulate and Supervising cybersecurity is the Cybersecurity Act B.E. 2562, which came into effect on May 28, 2019. The reason for enacting this Act is that currently, the provision of services or applications of computer networks, the Internet, telecommunications networks, or normal satellite services are at risk from cyber threats that may affect national security and peace and order within the country. Therefore, in order to prevent or deal with cyber threats in a timely manner, this law has been issued.
2. Infrastructure development: Thailand has established the Cyber Threat Monitoring and Response Center, Thai-CERT, to monitor the risk of cyber threats,

track, analyze and process information about cyber threats and cyber threat alerts, and NCSA- CERT to support activities in monitoring indicators related to cyber security.

3. Cooperation

a. International cooperation

Thailand has joined international organizations such as the ASEAN Cybersecurity Cooperation to enhance cooperation and coordination on cybersecurity in the ASEAN region, especially in strengthening cooperation on information and communication technology, and INTERPOL, where Thailand is a member of INTERPOL. In terms of cooperation on cybersecurity, INTERPOL supports the development of the potential of Thai police in dealing with cybercrime. There are joint training and exercises (Cybercrime Training Programs) to increase Thailand's potential to deal with cyber threats.

b. Domestic cooperation

Thailand has collaborated with the government, private sector, and the public, and has developed joint practices such as ISO 27001, an international standard that sets a framework for data security management, focusing on preventing risks that may occur to an organization's data. Thailand has used it in banks, telecommunications companies, etc., and the development of NIST, a guideline for cybersecurity management developed by (NIST

National Institute of Standards and Technology), which Thailand has used in government and private agencies related to security, such as finance, transportation, and energy.

4. Human resource development and understanding

Thailand has organized a training and development program for Cybersecurity personnel and has included Cybersecurity curricula in university and technical college education, such as the Master of Science in Cybersecurity and Information Assurance program at Mahidol University. It has also raised public awareness through campaigns and communications, such as the Think Before Click campaign initiated by the Ministry of Digital Economy and Society (MDES) in collaboration with various agencies, with the aim of reducing the number of incidents related to cyber threats.

RESULTS AND DISCUSSION

Results

Examples of cybersecurity development in Thailand

Establishing cybersecurity in Thailand is a process that involves the development and strengthening of cyber threat protection systems in many dimensions, including laws, technology, policies, and cooperation between the government, private sector, and the public. The following are the steps and examples that reflect the establishment of cybersecurity in Thailand in detail:

1. Development and enforcement of cybersecurity laws

Thailand has enacted laws to establish strong cybersecurity, especially to protect personal data and prevent cybercrimes related to computers and digital technology. The important examples of laws are as follows:

a. Personal Data Protection Act B.E. 2562 (PDPA):
    1) Description: This law stipulates regulations on storage and use of personal data, such as personally identifiable information, which must have data security measures to prevent leakage or breach of personal data.
    2) Example: If any organization collects personal data of citizens, such as ID card information or financial information, it must be stored securely, such as by encrypting the data, and must have data access checks to prevent unauthorized access.
b. Computer Crime Act B.E. 2550:
    1) Description: This law stipulates penalties for computer crimes, such as hacking, data hacking, and releasing viruses. Or actions that damage data
    2) Example: If someone breaks into a bank or company's system and steals customer data, they may be prosecuted under this law, which carries severe penalties of both imprisonment and fines.
c. National Cyber Security Act:
    1) Details: This law establishes agencies responsible for coordinating and managing cyber issues, such as creating a national cyber security plan and creating measures to deal with various cyber threats.
    2) Example: Establishing the National Cyber Security Center (ThaiCERT) that is responsible for alerting government and private agencies about cyber threats.

2. Establishing and strengthening cyber security agencies

Thailand has established agencies responsible for protecting the country's data and cyber systems, such as:

a. National Cyber Security Center (ThaiCERT):
    1) Details: It is a center responsible for dealing with cyber-attacks, coordinating between different agencies, and providing advice on cyber threat management.
    2) Example: ThaiCERT has notified organizations about cyber vulnerabilities, such as installing new threat protection systems or updating software to prevent hacker attacks.
b. Electronic Transactions Development Agency (ETDA):
    1) Details: ETDA is responsible for setting and overseeing electronic transaction standards, including creating online security.
    2) Example: ETDA has issued guidelines for establishing cyber security standards for business organizations, such as using data encryption, setting strong passwords, securing online financial transactions.

3. Creating a framework and standards for cyber threat prevention

Thailand has developed a framework and international standards that organizations must implement to maintain cyber security:

a. ISO/IEC 27001 (Information Security Management System):
b. Description: This standard provides organizations with guidelines for managing risks and preventing cyber threats in their information systems.
c. Example: Government and private organizations, such as banks or telecommunications companies, often use this method to manage customer data. There will be strict risk and access checks to prevent personal data from being leaked.

4. Prevention of Ransomware Attacks:
   a. Description: Ransomware is software that attacks by encrypting data and asking for a ransom to unlock it.
   b. Example: In response to this threat, the Ministry of Digital Affairs and related agencies have provided advice and training to the private and public sectors in the use of protection tools, such as regular backups and installation of anti-virus software that can detect new threats.
5. Cooperation between the government, private sector, and the public Cybersecurity cannot be done by the government or private sector alone.

   However, effective collaboration between various sectors is required:
   a. Public-private sector information exchange: Government agencies often collaborate with the private sector to exchange information related to cyber threats, such as alerts of potential attacks.
      1) Example: ThaiCERT coordinates with private organizations to alert about cyber threats that have a national impact, such as hacker attacks that may affect public services.
   b. Public education: Training and dissemination of knowledge to the public on threat prevention, such as using secure passwords, being careful about disclosing personal information online.
      2) Example: Creating online courses or cyber education campaigns to teach the public how to protect themselves from online scams (phishing) and other cyber-attacks.
6. Development and use of modern technologies to prevent cyber threats

Thailand has emphasized the use of new technologies to respond to increasingly sophisticated cyber threats, such as:

   a. Using AI and Machine Learning to detect threats: These technologies can help detect abnormal behavior in the system and provide real-time warnings.
      1) Example: Companies or government agencies use AI-based systems to detect potential hacking attempts or cyber-attacks on the network.

The Importance of building cybersecurity in Thailand

Establishing cybersecurity in Thailand is extremely important in the digital age where every aspect of people's and organizations' daily lives is linked through

information technology. The development and expansion of the digital economy has required Thailand to prepare for complex and diverse cyber threats, such as cyber-attacks that could affect the security of the country's critical infrastructure, such as the financial system, energy system, transportation system, or public health services. If attacked, it could cause damage to both operations and economic and social security. In addition, the security of personal data is a factor that cannot be overlooked because personal data is very valuable in an era where the online world is relied on for all activities. If there is a leak or attack, people will lose confidence and cause damage that could lead to problems with trust and digital transactions. Therefore, establishing cybersecurity is about protecting personal data from unauthorized access and reducing the risk of data being misused. Maintaining cybersecurity also protects industries and businesses from cyber threats that could affect the confidence of customers and partners, as well as reducing the risk of losing digital assets or important data of organizations, which will affect business operations and the ability to compete in the global market in an era where technology is increasingly used in operations. It also affects the enhancement of state security and government management. Protecting data related to governance and state operations is important to prevent important data from being stolen or destroyed by cybercriminals, which could lead to instability at both the political and national security levels. Therefore, building cybersecurity plays an important role in promoting trust in the digital system, which is a key factor in driving the digital economy and national development. If citizens and organizations are confident in the security of their data and online transactions, it will help the growth of the digital economy to be stable and sustainable.

Finally, international cooperation in dealing with cyber threats is also important because today's cyber threats are often cross-border. Exchanging threat information and international cooperation strengthens cybersecurity at the international level and helps reduce threats that may affect both the country and the region.

Therefore, building cybersecurity in Thailand is an important factor not only in terms of protecting data and assets, but also in promoting economic and social security for the country in the digital age, which will be an important foundation for creating stability and prosperity in the future.

Highlights or Achievements

Highlights and achievements in cybersecurity in Thailand are as follows:

a. Enforcement of the Personal Data Protection Act (PDPA) by officially enacting the Personal Data Protection Act (PDPA) in 2022, which protects the personal data of citizens and builds confidence in all sectors. This law requires all organizations to have transparent and secure data management measures.
b. Development of the National Cyber Security Plan: Thailand has developed the "National Cyber Security Master Plan 2022-2027", which covers all dimensions of cybersecurity protection, supports the development of human potential in cybersecurity, and aims to promote cooperation with other countries to exchange information on threats.

c. Establishment of a specialized agency for cybersecurity: Thailand has established the National Cyber Security Agency (NCSA), which acts as a center for preventing and responding to cyber threats in Thailand and promotes cooperation between the public and private sectors.
d. Creation of the Cybersecurity Monitoring System (ThaiCERT): Thailand has created the ThaiCERT (Thailand Computer Emergency Response Team) system as a cybersecurity monitoring center in the country, which monitors cyber threats in real time and provides advice and solutions to cybersecurity issues for various agencies.

Things that need to be developed in Thailand's Cybersecurity

1. Lack of cybersecurity skills and human resources

Despite the development and knowledge of Cybersecurity, Thailand still lacks experts and personnel with sufficient knowledge in this field, both at the government and private sector levels.

Issue: There are still not enough cyber experts, causing the ability to fully respond to complex threats.

2. Lack of awareness of cybersecurity

Despite the dissemination of knowledge about Cybersecurity, most people are still not aware of the importance of protecting personal data and using technology safely.

Issue: The public's knowledge of Cybersecurity is still not very widespread, creating a risk channel for being attacked by various threats such as Phishing or online fraud.

3. Gaps in cybersecurity measures in the private sector

Some organizations have not yet installed adequate security measures. Although there are standards such as ISO/IEC 27001, some organizations may not strictly implement the standards or conduct audits.

Issue: Some private sectors still lack investment in modern threat prevention systems or the development of effective response plans.

4. Cybersecurity threats are evolving rapidly

In particular, the use of new techniques such as AI-driven attacks or threats that use unknown vulnerabilities (Zero-day Vulnerabilities)

Issue: Adapting to rapidly evolving threats is a major challenge, as there may be gaps in the defense system that have not yet been fixed.

5. Challenges in coordination between government agencies

Although cybersecurity policies and measures have been developed in Thailand, there are still challenges in coordination between different government agencies and in developing systematic measures.

Issue: Coordination between government agencies responsible for cybersecurity is still incomplete, which sometimes makes it impossible to respond to threats at the national level in a timely manner.

Discussion

Building cybersecurity in Thailand and the International context

Thailand's cybersecurity and the international context share many similarities, with both countries focusing on preventing cyber threats and building security in a globally connected digital world. Despite differences in some areas related to laws, cultures or levels of development, there are important commonalities in cybersecurity strategies and approaches, as follows [8]:

1. Establishing a Cybersecurity Policy and Legal Framework
    a. Thailand: Several laws and policies have been enacted to maintain cybersecurity, such as the 2019 Cybersecurity Act, which focuses on preventing cyber threats, establishing security standards and establishing a centralized cyber coordination body.
    b. International context: Many countries, such as the United States and the European Union, have developed strong laws and policy frameworks to control and manage cyber threats, such as the US Cybersecurity Act or the EU GDPR, which focuses on the protection of personal data [9].
2. Establishing a coordination center and responsible agency (Cybersecurity Coordination Centers and Agencies)
    a. Thailand: There are agencies responsible for maintaining cybersecurity, such as the National Cybersecurity Agency (NCSA), which is responsible for setting guidelines and coordinating with other agencies.
    b. International context: Many countries have agencies or centers working on cybersecurity, such as the Cybersecurity and Infrastructure Security Agency (CISA) in the United States or the European Union Agency for Cybersecurity (ENISA) in the European Union, which act as a center for coordinating and responding to cyber threats [10].
3. Cyber threat management
    a. Thailand: There are Cybersecurity Operation Centers (COCs) to deal with cyber threats. Particularly in the government and critical sectors.
    b. International context: Countries are using advanced technologies and tools to monitor and manage cyber threats, such as Threat Detection Systems and sharing threat intelligence across organizations such as the Forum of Incident Response and Security Teams (FIRST) [11].
4. Education and training
    a. Thailand: Cybersecurity education and training has been promoted through the development of university-level education programs and training for officials and personnel working in this field.
    b. International context: Many countries have established specialized cybersecurity training programs and courses, especially in developed countries, such as cybersecurity training for experts and practitioners in organizations. Including raising awareness in the general society [12].

5. Cyber defense and response
    a. Thailand: Incident Response Plans have been developed to respond to cyber threats quickly and effectively.
    b. International context: Many countries have developed globally consistent cyber threat response plans, such as working with international organizations to address transnational threats or large- scale cyber attacks [13].
6. International cooperation
    a. Thailand: Cooperating with other countries in the Asia-Pacific region to maintain cybersecurity, such as through cooperation under the ASEAN framework.
    b. International context: Maintaining global cybersecurity often involves close international cooperation through organizations such as the United Nations (UN), the G7 Summit, and other relevant international organizations to address global cyber threats [14].
7. Data protection and privacy
    a. Thailand: The Personal Data Protection Act (PDPA) provides measures to protect personal data in maintaining cybersecurity.
    b. International context: Protecting personal data is an important issue worldwide, such as the EU's GDPR or the California CCPA. which has strict regulations for managing personal data and preventing data leaks or breaches [15].

Cybersecurity in Thailand and the international context differ in many dimensions, with key differences in laws, cyber threat management, technology investment, and international cooperation, as follows:

1. Legal framework and policies
    a. Thailand: Cybersecurity in Thailand has become more visible in recent years, with legislation such as the 2019 Cybersecurity Act, which focuses on establishing a regulatory body to systematically monitor and prevent cyber threats. There is also the Personal Data Protection Act (PDPA), which sets strict measures for the management of personal data.
    b. International context: In other countries, especially in developed countries such as the United States and the European Union, there are more stringent and comprehensive legal frameworks, such as the European Union's General Data Protection Regulation (GDPR), which has high levels of data retention and protection and is widely enforced. There is also the US Cybersecurity Information Sharing Act (CISA), which facilitates the smooth exchange of information on cyber threats between the public and private sectors.
2. Cyber threat management
    a. Thailand: Thailand has mechanisms for managing cyber threats at the state level, such as the establishment of a Cyber Security Operations Center. (Cybersecurity Operation Centers, COCs) to deal with potential cyber- attacks, but cyber threat response is not as robust as in many developed countries.

b. International context: Many developed countries, such as the United States and the European Union, have established highly effective response structures, such as the National Cybersecurity and Communications Integration Center (NCCIC) in the United States or ENISA (European Union Agency for Cybersecurity) in Europe, which are organizations that help coordinate cyber threat response, including exchanging threat information between countries and the private sector.

3. Investment in technology and resources
   a. Thailand: Investment in cybersecurity technology in Thailand is still not up to international standards in many areas, especially in terms of modern technology for detecting and responding to cyber threats. Even some government agencies lack sufficient investment in technology to deal with cyber threats.
   b. International context: Developed countries, such as the United States and the European Union, have invested in advanced technology and have developed tools that can detect and respond to cyber threats immediately, such as using AI systems to detect cyber threats or Blockchain to maintain data security.
4. Education and training
   a. Thailand: In Thailand, the promotion of cybersecurity education and training is still insufficient. Despite the development of cybersecurity education programs in universities and training for government personnel, knowledge and understanding in this area is not widespread throughout the country.
   b. International context: Developed countries such as the United States have established cybersecurity education and training programs at university and organization levels and have created collaborations between the public and private sectors to develop cyber skills for personnel. In addition, there are ongoing training and awareness programs for the public.
5. International cooperation
   a. Thailand: International cooperation in cybersecurity in Thailand is still in the development stage. Thailand has collaborated with other countries in the Asia-Pacific region and within the ASEAN framework to maintain cybersecurity.
   b. International context: Internationally developed countries have strong international cooperation, with international cooperation in sharing cyber threat information, such as FIRST (Forum of Incident Response and Security Teams) and cooperation under the UN or OECD framework, which has established rules and guidelines for international cooperation in solving cyber threats.
6. Data Privacy and Protection
   a. Thailand: Thailand has a PDPA (Personal Data Protection Act) that aims to protect personal data, but the law enforcement is still relatively new and not nationwide. There are gaps in monitoring and enforcement that need to be improved.

b. International context: Developed countries such as the European Union have implemented the GDPR, a strict data protection law with clear measures in place to detect data breaches and enforce them effectively.

CONCLUSION

Fundamental Finding : This study highlights that the establishment of cybersecurity in Thailand is a multifaceted effort involving legislative frameworks, institutional policies, human resource development, and international cooperation. The Cybersecurity Act of 2019 and related initiatives illustrate Thailand's proactive approach in addressing the growing risks associated with digital technology and personal data security. **Implication :** Effective cybersecurity not only safeguards personal data but also enhances public trust in digital systems, supports economic stability, and strengthens national security. The collective involvement of government, private sectors, and the public is essential in sustaining a resilient cybersecurity ecosystem. **Limitation :** However, the study is limited by its reliance on secondary data and lacks empirical evidence on the implementation effectiveness across different regions and sectors in Thailand. **Future Research :** Further studies should involve primary data collection, including stakeholder interviews and case studies, to evaluate the real-world impact of cybersecurity policies, identify systemic gaps, and propose adaptive strategies for evolving cyber threats in the context of digital transformation.

REFERENCES

[1] H. Runowski, "The role of digital technologies in building trust in agriculture," in *Trust, Organizations and the Digital Economy*, Routledge, 2021, pp. 187–201. doi: 10.4324/9781003165965-15.

[2] D. W. Schartum, "Sharing information between government agencies: some legal challenges associated with semantic interoperability," in *Innovating Government*, T. M. C. Asser Press, 2011, pp. 347–361. doi: 10.1007/978-90-6704-731-9_19.

[3] K. Bogatyrev, "Trash content as a form of information threats to media security in the digital environment," *Legal Linguistics*, no. 24 (35), pp. 38–44, Jul. 2022, doi: 10.14258/leglin(2022)2407.

[4] I. Alsmadi, "Information systems security management," in *The NICE Cyber Security Framework*, Springer International Publishing, 2020, pp. 31–53. doi: 10.1007/978-3-030-41987-5_2.

[5] M. Kumaran, "Case studies on the integration of 5G technology into smart grids with emphasis on cybersecurity measures," in *5G and Fiber Optics Security Technologies for Smart Grid Cyber Defense*, IGI Global, 2024, pp. 424–435. doi: 10.4018/979-8-3693-2786-9.ch019.

[6] M. Abdirisak Buraale, T. Khawa Abdurrahman, and F. Che Fauzi, "Assessing cybersecurity threats and awareness in bosaso's banking and telecom sectors," *International Journal of Science and Research (IJSR)*, vol. 13, no. 8, pp. 738–747, Aug. 2024, doi: 10.21275/sr24810182035.

[7] F. Skopik, G. Settanni, and R. Fiedler, "The importance of information sharing and its numerous dimensions to circumvent incidents and mitigate cyber threats 1," in

Collaborative Cyber Threat Intelligence, Auerbach Publications, 2017, pp. 129–186. doi: 10.4324/9781315397900-4.

[8] N. K. Chaudhary, "Cybersecurity threats mitigation and preventive strategies amid COVID-19 pandemic," *NFSU Journal of Cyber Security Digital Forensic*, vol. 2, no. 1, 2023, doi: 10.69490/jcsdf720250526.

[9] A. Bendiek and E. Pander Maat, "The EU's cybersecurity policy: building a resilient regulatory framework," in *Cybersecurity and Legal-Regulatory Aspects*, WORLD SCIENTIFIC, 2021, pp. 23–64. doi: 10.1142/9789811219160_0002.

[10] G. Christou, "Network and information security and cyber defence in the European Union," in *Cybersecurity in the European Union*, Palgrave Macmillan UK, 2016, pp. 119–143. doi: 10.1057/9781137400529_6.

[11] C. Easttom, "Threat analysis," in *The NICE Cyber Security Framework*, Springer International Publishing, 2020, pp. 207–228. doi: 10.1007/978-3-030-41987-5_10.

[12] G. O. Hasanova, "The principle of education humanisation: training pedagogy personnel," in *THE PRINCIPLE OF EDUCATION HUMANISATION: TRAINING PEDAGOGY PERSONNEL*, ICSP "NEW SCIENCE," 2024. doi: 10.46916/28082024-978-5-00215-505-7.

[13] S. Guduru, "Autonomous cyber defense: LLM-Powered incident response with LangChain and SOAR integration," *International Journal of Science and Research (IJSR)*, vol. 10, no. 5, pp. 1378–1382, May 2021, doi: 10.21275/sr21059083032.

[14] G. Lo Brutto, "International cooperation," May 2022, *Routledge*. doi: 10.4324/9780367565152-rechs75-1.

[15] M. Brkan, "Privacy, data protection and the role of European Courts: towards judicialisation and constitutionalisation of European privacy and data protection framework," in *Research Handbook on Privacy and Data Protection Law*, Edward Elgar Publishing, 2022, pp. 274–302. doi: 10.4337/9781786438515.00022.

*** Thipphawan Poonsawat (Corresponding Author)**
Burapha University, Thailand
Email: thipphawanpoonsawat@gmail.com