Cybersecurity Policy in ASEAN Countries

Jirapon Sunkpho, Sarawut Ramjan, Chaiwat Ottamakorn
Thammasat University
jirapon@tu.ac.th, sarawut@citu.tu.ac.th, chaiwat@citu.tu.ac.th

Abstract

Implementing cyber security policy is challenging for every country. The government of ASEAN countries have implemented cybersecurity policy and legislation to ensure the openness of the internet platform to boost innovation and economy while maintaining security in cyber space as well as protecting its citizen's personal information and privacy from being misused. Several measures and actions were developed and being enacted. This paper gave an overview on recent legislative and policy developments pertaining to the cybersecurity and data protection in ASEAN countries with focusing on the detail policy of 6 major ASEAN countries including Indonesia, Malaysia, Philippines, Singapore, Thailand, and Vietnam. The paper also suggest more collaboration among ASEAN countries to cambat with growing cyber threats.

Introduction

Internet have become an integral part to the nation's competitiveness and to the well-being of its citizen. This is because internet and ICTs are essential for economics and social development and form a vital infrastructure for a country [OECD 2012]. A World Bank study using a panel of 120 countries concluded that a 10 percent point increase in broadband penetration results in a 1.38 percent increase in annual GDP growth in developing countries and 1.21 percent in a developed country [Qiang and Rossotto, 2009].

ASEAN is becoming one of the fastest growing region in the world with the population of 634 million (over 100 million more than the European Union). It is the third most populous market in the world and with the combined GDP of more than $2.55 trillion making ASEAN the world's seventh largest economy [ASEANstats, 2018]. A study by ATKearney indicating that digital economy could add 1 trillion USD to the GDP of the region which could boost the GDP of the region by 35% [ATKearney, 2018]. However, the "digital economy" which heavily relies on technology for business transactions opens an avenue for new threats such as online fraud, hacking and distribution of inappropriate materials. Deterring cybercrime is therefore, necessary for national security and protection of the information infrastructure. It is therefore a priority for legislators to adopt proper legislation to prevent the use of information and communication technologies for criminal activities. The challenge is for governments to make the use of the technology safer without minimizing the developmental opportunities.

An analysis by ATKearney indicated that ASEAN countires have emerged as a prime target for cyberattacks for several reasons [ATKEarney, 2018] due to the following reasons. First, ASEAN countries especially Malaysia, Indonesia, and Vietnam have emerged as global host spots for major blocked suspicious web activities. Secondly, the region's policy, governance, and cybersecurity capabilities is relatively low. Third, there is shortage of home-grown capabilities and expertise due to fragmented industry and shortage of skilled talent. Fourth, perception of cyber risk from corporates stakeholders do not see cybersecurity as business priority resulting in the absence of holistic approach to cyber resilience. Finally, breath of security product landscape and fragmentation of vendor solution results complexity in the operation of companies in the region. A study by Ponemon Institute suggests that it takes on average of 184 days to identify data break and close to 65 days to contain it for ASEAN companies [Ponemon, 2017].

Governments in ASEAN countries have tried aims to strengthen cyber security for the Internet economy to further drive economic. They also must preserve the openness of the Internet and fundamental values which is another key consideration that the government should carefully manage. Thus it is the aim of this paper to revisit its cyber security strategies and legislation of ASEAN countries.. In this paper, legislative

approach to meet these three objectives by ASEAN countries were reviewed and then finally summarized the similarity and differences among ASEAN countries.

Cybersecurity Policy Goals

In order to ensure public trust on performing transaction online, most governments in ASEAN countries have developed cybersecurity policy with the purposes of three specific goals: Ensuring open internet to promote Innovation; Combating Cybercrime; and Ensuring Privacy of their citizen.

First and foremost, the government should ensure the openness of the internet platform so that innovation can be flourished in the digital economy. Platforms have been critical to innovation as they facilitate various forms of commerce transaction e.g. allowing small merchant to reach global market. Platforms also enable free speech and economic productivity because new products and services can be built cheaply and at scale. According to Accenture, platform economy represents around 2.6 trillion USD in the market capitalization worldwide [Accenture, 2016]. Openness of the platform is essential since it allows "permission-less innovation" where citizens can develop products or services without asking permission from the platform owners. Thus, the key protection that the government need to provide to internet platforms is liability limitation meaning that those who operate internet platforms can decide not to worry about certain potential legal liabilities, and just concentrate on running their service.

Secondly, the government should ensure the safety of the internet by making sure that traffic that flows across the internet has basic features of confidentiality and integrity by protecting the citizen from cybercrime activities such as stealing files or breaking into other computer systems. A study by UK government indicates that estimate cost of cyber crime to the UK citizens is 3.1 billion pounds per year and about 2.2 billion to the government [Gov.uk, 2011]. As a result, it is essential for countries to ensure safety and integrity of the internet by formulating a set of legislation to combat with cybercrime such as identity theft and online scams.

Finally, government should ensure privacy of their citizen by making sure that their private behavior or their personal data should be protected and should not be used against them. Since, the internet economy is going to depend on personal data, individual may feel threatened by the fact that some of their personal information will be used or their behavior will be under surveillance. There are four approaches for the government in handling privacy issue: 1) statutory general data protection laws e.g. European Union's Data Protection Directive, (2) sector-specific laws (such as for medical or financial information), (3) stateapproved guidelines, and (4) a self-regulatory approach, as represented by the US (though that country includes some sector-specific restrictions) [Inter-Pacific Bar Association, 2001]

ASEAN Cybersecurity Legislation Landscape

According to 3 specific goals of cybersecurity policy, table 1 summarized the legislation efforts of 6 major countries in ASEAN (ASEAN-6). In term of ensuring openness of the platform, methods of Notice and takedown and Judical system were used. For cybercrime prevention, several cybersecurity laws have been enacted. Finally, there are laws and regulation about data protection which will help ensuring the use of data user to conform with certain rules and standards. The following paragraph explains cybersecurity policy approach in more detail.

Indonesia

Government of Indonesia has conducted a series of efforts to protect cyberspace from the threat of cybercrime. One of the Government's efforts in protecting the security of information in cyberspace is by publishing the Telecommunication Act (UU Telekomunikasi No. 36/1999) and Information and Electronic Transaction Act (UU ITE No. 11/2008). These are the two acts that become the basic foundation for formulating regulations and policies related to information security. Just recently, Indonesian government established the National Cyber and Encryption Agency (BSSN) in which its main responsibility is to prevent cyber attacks as well as to respond with an urgent strategy. The agency will

also work towards strengthening country's defense against cyber threats and increasing public awareness on cybersecurity [Kelleher, 2017].

	Openness of the Platform	**Cybercrime Prevention**	**Privacy**
Indonesia	Judicial System	No Specific cybersecurity laws; Information and Electronic Transaction Act (Law of the Republic of Indonesia No. 11 of 2008)	Data Protection Regulation (2016) -Personal Data Protection (Draft)
Malaysia	Notice and takedown	Computer Crime Act 1997	Personal Data Protection Act 2010 (PDPA).
Philippines	Judicial System	Cybercrime Prevention Act (2012)	Data Privacy Act (2012)
Singapore	Notice and takedown	COMPUTER MISUSE ACT (1993, amended 2017)	The Data Privacy Act of 2012
Thailand	Judicial System	Computer-Related Crime Bill (2007, amended 2017))	Sector specific approach such as National Health Service Act -Personal Information Protection Act (Draft)
Vietnam	Judicial System	Law on Cyber Information Security (Law No. 86/2015/QH13)	Law on Cyber Information Security (Law No. 86/2015/QH13)

Table 1 Summary of cybersecurity legislation based on 3 cybersecurity policy goals

For personal data protection and privacy issue, the Minister of Communication and Informatics (MOCI) issued a Personal Data Protection in Electronic Systems (MOCI Regulation 20) which is a guideline under the Information and Electronic Transaction Act. The House of Representatives is also now in the process of drafting a new law on Personal Data Protection (PDP Draft Law). The enactment of the PDP Draft Law would be the first comprehensive law in Indonesia that specifically deals with the personal data protection [Rahmansyah and Tahir, 2017].

Malaysia

Malaysia has a range of existing legislations dealing with the cyber environment. However, the law that is used to combat with cyber threats is the Computer Crimes Act (CCA) 1997 [MCCA 2017]. CCA has been created to provide offenses relating to the misuse of computers and to complement existing criminal laws (Annamalai, 1997). For personal data protection issues, the Personal Data Protection Act 2010 (PDPA) was used to protect personal data from being misused. It operates based on 7 principles namely: General, Notice and Choice, Disclosure, Security, Retention, Integrity, and Access Principle. Personal data is defined as any information collected or processed in connection to a commercial transaction by any equipment operating automatically and is capable of identifying a person. The above definition will include such information as names, addresses, identification card/passport numbers, email addresses, telephone numbers, as well as banking details [PDPCM, 2013]. The law, however, only applies to the processing of personal data in commercial transactions but does not apply to the federal government of Malaysia or to its state governments [Hunton and Williams,2013].

Since CCA and PDPA has been enacted since 1997 and 2010 respectively. There are some cyber activities that have not been addressed by these laws e.g. Denial-of-service or Phishing. As a result, Malaysian Government is in the process of introducing a new law that is aimed to cope with these new cybersecurity threats. The proposed law will empower the National Cyber Security Agency (NCSA) to be the coordinating agency to deal with cybercrimes, terror operations, and money laundering [TMI, 2017].

Philippines

On 2012, Philippines government crafted Cybercrime Prevention Act defining cybercrime (Republic of the Philippines congress of the Philippines, 2012). This act provided for the prevention, investigation, suppression and the imposition of penalties therefore, and for other purposes. This act only defines a characteristic of cybercrime and punishment, but also guide a law implementation. Following the act, the government established Philippine Office of Cybercrime (Department of Justice, 2018) which has authority to investigating and prosecution of cybercrimes and facilitating an international cooperation.

Philippines also passed the Data Privacy Act 2012, which is a comprehensive and strict privacy legislation. The law (1) protects the privacy of individuals while ensuring free flow of information to promote innovation and growth; (2) regulates the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of personal data; and (3) ensures that the Philippines complies with international standards set for data protection through National Privacy Commission" [National Privacy Council, 2012].

Singapore

Singapore takes cybersecurity threats seriously and has set up the Cyber Security Agency of Singapore (CSA) as the central agency to oversee and coordinate all aspects of cybersecurity for the nation [CSA, 2017]. The main legislation dealing with computer crimes in Singapore is the Computer Misuse Act 1993 (CMA). The Computer Misuse Act (CMA) was enacted in 1993 to criminalize unauthorized access or modification of computer material, and other computer crimes. The Act was amended twice between 1994 and 2013 to, amongst other things, introduce new offences to keep pace with changes in criminal behavior. In 2013, the CMA was amended to include cybersecurity measures and renamed the Computer Misuse and Cybersecurity Act (CMCA). In 2017, The Singapore Parliament just passed amendments to the existing Computer Misuse and Cybersecurity Act. The amendments are designed to address to tackle the increasing scale and transnational nature of cybercrime, as well as the evolving tactics of cybercriminals [MHA,2017].

In dealing with personal data and privacy issues, Personal Data Protection Act 2012 (PDPA) was enacted and it comprises of rules governing the collection, use, disclosure and care of personal data. It also recognizes both the rights of individuals to protect their personal data e.g. rights of access and correction, and the needs of companies to collect, use or disclose personal data for legitimate and reasonable purposes. The establishment of national Do Not Call (DNC) Registry was also the result of PDPA. The DNC allows residents of Singapore to register their telephone numbers to opt out of receiving marketing phone calls, SMS or MMS, and faxes from companies. [PDPC, 2018]

Thailand

In recent years, the Thai government has pledged support for the promotion of Thailand's information and communications technology (ICT) sector, with a series of strategies aimed at developing related infrastructure, accelerating innovation, and transforming the country's economy into one that is based on digital technologies. In addition, the country's Cabinet officially approved a project titled "Thailand Economy 4.0" aims to move Thailand's economy to the next level by facilitating the trade in goods and services through e-commerce (MICT, 2016).

As part of the plan, Ministry of Information and Communication Technology (now the Ministry of Digital Economy and Society) proposed the adoption of eight items of legislation, to support development of the digital economy. Of those eight items, the most controversial law is the amendment of the ComputerRelated Crime Bill that allows the government to shut down websites and penalize internet service providers who fail to remove any content that considered as illegal or sensitive [HRM, 2016]. As for personal data protection at present, Thailand does not have any general statutory law governing data protection or privacy. However, the Constitution of the Kingdom of Thailand does recognize the protection of privacy rights and there are laws in some sectors such as The Financial Institution Act and the National Health Service Act do provide a certain level of protection against any unauthorized

collection, processing, disclosure and transfer of personal data [DLA, 2017]. The draft Personal Information Protection Act ('Draft'), which has been reviewed by the Council of State, provides protection of personal data by restricting the gathering, using, disclosing and altering of any personal data without the consent of the data owner. The Draft also imposes both criminal penalties and civil liability for any violation of the Draft and calls for the establishment of a Protection of Personal Data Commission to regulate compliance with the Draft. [DLA, 2017].

Vietnam

Vietnam has developed a law on e-Transaction on 2005 and just enforce a new Law on Cyber-Information Security (LCIS). LCIS was passed by the National Assembly of the Socialist Republic of Vietnam on November 19, 2015, and it was enacted since July 1, 2016. It is the first comprehensive law ever issued in Vietnam on the security of "cyber-information in which its main purpose of is to dealing both security and integrity of the internet network as well as to protect of personal information in the network environment. The law sets out a system to classify digital information and specify the steps public organizations need to follow to protect such data. It mandates the Ministry of Communication and Information (MCI) and the Vietnam Computer Emergency Response Team (VNCERT) as the leaders in the nation's battle against cybercrime [Socialist Republic of Vietnam, 2015].

Summary and Conclusion

The survey of cybersecurity policy and legislative of 6 ASEAN countries have been reviewed. As one can see, most countries in ASEAN have achieved some forms of legislation and policy to handle the issues of openness of the platform by providing limited liability of platform owners, combating cybercrime by providing a law that punish the wrong doing in the internet, and taking care of citizen personal data by providing laws and regulation to ensure the privacy of the citizen. However, the level of the development and the content of each legislation and policy are not treated equally. In term of limited liability, only Singapore and Malaysia that have Notice and Takedown procedure in place. Indonesia, Philippines, Thailand, and Vietnam do not provide legal provisions for a Rights Holder to directly enforce their copyright protections through an ISP notification system, and are instead forced to seek copyright enforcement through legal action or as referred by "Judicial System."

All 6 ASEAN countries studied in this paper have some form of legislation dealing with cybercrime. Only Indonesia that do not have specific cybersecurity law but rely on the electronic information and transaction act. On the issue of data protection, all countries with Thailand and Indonesia being the exception do have general data protection law in place. Thailand and Indonesia do not have a unified law regarding privacy, instead, it is informed by different laws and decrees. However, both Thailand and Indonesia are in the process of drafting a new general data protection law. Vietnam is the only country that have a comprehensive law that dealing with both security and data protection in one single law of Cyber-Information Security (LCIS). One interesting point to note is that Malaysia only applies the Personal Data Protection Act to commercial transactions excluding data processed by the government.

The issue that should be addressed among ASEAN countries is collaboration since collaboration and information sharing is indeed a vital aspect of cyber security. Without collaboration, siloed cyber security ecosystems are easily compromised [Tan, 2018]. One of the collaboration effort that can be done is by establishing a regional cybersecurity coordination platform that will be used to coordinate and sharing of information and intelligence on cyber incidents among countries in ASEAN as well as making it one of the regional policy agenda [ATKearney, 2018].

References

Accenture (2016). Platform Economy: Technology-Driven Business Model Innovation from the outside in. Source: https://www.accenture.com/fr-fr/_acnmedia/PDF-2/Accenture-Platform-EconomyTechnology-Vision-2016-france.pdf. Retrieved Feb 15, 2018.

Appudurai J. and Ramalingam C. (2007). Computer Crimes: A Case Study of What Malaysia Can Learn from Others? The Journal of Digital Forensics, Security and Law. Vol. 2 No.2

ASEANstats (2018). http://www.aseanstats.org/

ATKearney (2018). Cybersecurity in ASEAN- AN Urgent Call to Action. Source: https://www.cisco.com/c/dam/m/en_sg/cybersecurity/cybersecurity-inasean/files/assets/common/downloads/publication.pdf Retrieved: Feb 15, 2018.

CSA (2017). MCI and CSA seek Public Feedback on Proposed Cybersecurity Bill. https://www.csa.gov.sg/news/press-releases/mci-and-csa-seek-public-feedback-on-proposed-cybersecuritybill. Retrieved Feb 18, 2018.

Department of Justice. (2018). "Philippines Office of Cybercrime", Source: https://www.doj.gov.ph/office-ofcybercrime.html Retrieved 11 February 2018.

DLA (2017) . Data Protection Law of the World- Thailand. Source: https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw.data_protection/fu nctions/handbook.pdf?country-1=TH

Gov.uk (2011) The Cost of Cybercrime. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60942/THECOST-OF-CYBER-CRIME-SUMMARY-FINAL.pdf

Hunton and Williams (2013) , Malaysian Data Protection Law Takes Effect. Source: https://www.huntonprivacyblog.com/2013/11/19/malaysian-data-protection-law-takes-effect/ Retrieved 15 Febuary 2018.

HRM (2016) . Thailand: Cyber Crime Act Tightens Internet Control. Source: https://www.hrw.org/news/2016/12/21/thailand-cyber-crime-act-tightens-internet-control Retrieved Feb 18, 2018.

Inter-Pacific Bar Association (2001). Privacy and Data Protection Issues in Asia. Source: https://ipba.org/media/fck/files/elawasia_ipba_privacy.pdf Retrieved Feb 15, 2018.

Kelleher J. (2017) , " Indonesia Launches Cyber Security Agency" , Source: https://www. opengovasia. com/ articles/ 6563-indonesia-launches-cyber-security-agency-in-wake-ofgrowing-threat-landscape Retrieved: 9 February 2018.