International Journal of Global Community
Volume V No.1 (March), 2022

Cybersecurity Regulation and Governance During the Pandemic Time in Indonesia and Singapore

Awaludin Marwan
Bhayangkara Jakarta Raya University
Email: awaludin.marwan@dsn.ubharajaya.ac.id

Jiow Hee Jhee
Singapore Institute of Technology
Email: jhee.jiow@singaporetech.edu.sg

Kevin Monteiro
Singapore Institute of Technology
Email:kevinmonteiroh@gmail.com

Abstract

Discussing the cyber security regulation in Singapore and Indonesia, which delineating the role of cyber security agency and the cyber security policy in the era of pandemic is a pivotal component. Cyber security can investigate cyber incident which involved many victims and sensitive data. For instance, in June 2018, hackers breached the 1.5 million patient's data of the SingHealth IT systems. In Indonesia, it was happened the data breach involved the voter personal data of general election. Despite, the agency had failed to arrest the cyber criminals, the prevention and reparation of IT security system in the critical infrastructure and public electronical good is very important. During the pandemic, people use the internet more and need to be secured.

Keywords: cybersecurity regulation, Indonesia, Singapore, data breach

RIKSAWAN INSTITUTE®

Introduction

Veronis (2020), a data security company has shown that the data breach occurred approximately 7 million every day. The data breach may cost around $ 3.86 million in accordance with the Global Cost a Data Breach Report by IBM in 2018. Moreover, during the pandemic the cyber incident increased over time. Cyber-attacks such as brute-force towards servers were up 23 % in April 2020, malicious codes were transplanted on application increased by 8 % in April, and network attack and phishing escalated since quarter first 2020 (Tan, 2020). Even more, cybercriminals, in some occasions, are trying to attack the healthcare system in the pandemic time. Herewith, the analysis of cybersecurity policy in the pandemic time is an important component to delineate the effectiveness of cyber incident prevention.

This paper will discuss the condition of cyber security policy in Indonesia and Singapore. At the global level, Singapore occupies the 6th of cyber security index and Indonesia is on the 41st from 175 countries around the world in accordance with the ITU publication of 2018. In this study, we compare how similar and different are the cybersecurity laws and practices between Indonesia and Singapore. As such, a discussion on the legal system and social analysis related to cybersecurity in both countries will ensure, especially during the pandemic time when such issues are more pronounced.

Singapore: Cybersecurity Act (2018)

The Cybersecurity Act (CSA) came into force on 31 Aug 2018, with the primary aim of "enhancing Singapore's cyber security landscape and strengthening the city state's ability to routinely protect the nation's Critical Information Infrastructure [(CII)]" (Kok & Cheang, n.d.). CII includes elements such as databases, network, communications infrastructure that are under the control of the State (Emma-Iwuoha, 2017) which are increasingly fundamental components for the operation of all other government sectors (Lopez, Ray and Crispo, 2012). In the next following parts of the essay, we will delve into why it was enacted and whether or not previous (or existing laws) were/are adequate enough to handle the problems that Singapore was facing with regards to cyber security.

Why was it enacted? There were several reasons for the CSA to come into fruition.

Firstly, it was enacted to bolster digital security and digital resiliency measures in industries responsible for providing essential services (KPMG, 2019). CII are computer components that are directly involved in the provision of essential services; the act was enacted to help design a framework for how CII is designed and grants CII owner's clarity on their specific obligations to protect their systems from cyberattacks (Ministry of Communications and Information, 2018).

Secondly, the CSA provided for a delegation of structured authority; it authorizes the "commissioner of cybersecurity to investigate cybersecurity threats" so as to prevent cybersecurity incidents from causing further harm and pre-empt future events (CSA, 2018). Essentially, this allows for powers to be exercised according to the severity of the cybersecurity threat, in order to not only assure Singaporeans of safety in terms of cybersecurity, but will also ensure that resources are utilised efficiently and not left to idle into complacency as this would lead to major lapses that result in significant attacks. The biggest example of a major lapse would be when, in June 2018, hackers stole the data of 1.5 million patients via the SingHealth IT systems due to employees ignoring signs of a potential breach and vulnerabilities within the system (Loh, 2019). Enacting the CSA primarily seeks to stop such a prominent attack from ever resurfacing on our country, by detailing the responsibilities of the stakeholders.

The increase of cybersecurity demands can result in an entanglement of government and public sector responsibilities (Wyman, 2019). This can lead to important data being relatively difficult to properly and thoroughly disseminated given that there are multiple channels, procedures and systems in place between the government and public sector that may distort them significantly. The enactment of CSA it will allow for this dissemination process, which involves communications and decisions to be recorded via appropriate company systems (Uliginn and Hayes, 2020), to be more useful for the government and owners of computer systems to identify and recognize vulnerabilities, which efficiently deters cyber-related incidents (CSA, 2018).

This act also brings about the provision of a structured licensing framework for service providers that perform penetration testing and managing security operation centre monitoring (CSA, 2018). Because they have access to sensitive information from clients, and are relatively mainstream in the market, licensing will help to balance security needs whilst developing the country’s cybersecurity ecosystem safely (CSA, 2018).

Singapore, with how fast she has grown and developed into a cosmopolitan country, has developed a hyper-connected business hub which, while impressive, does make it prone and vulnerable to cyberattacks that continue to increase in scale and sophistication. For instance, in 2017, the army headquarters “MINDEF” suffered a massive data leak that affected 850 people (Chua, 2017). Such an example of a leak, is one of the reasons why this act has been enacted as a form of safeguarding and a display of forward-minded thinking in order to be prepared for future cyber breach attempts. As a result of the act, CII owners are now better equipped if such cases were to ever reoccur (CSA IFAQ, 2018) as the regulation “professionalises the industry at a time where more organisations are searching for and consuming cybersecurity services” (CSA IFAQ, 2018); now, CII owners will have wider access to resources and assistance from more organisations which can render them more capable if there were to be a future cyber breach attempt aimed at them.

Prior to CSA, CII owners were actually not given clear duties. Now, with the CSA, they have a variety of statutory duties such as “notifying change in data ownership, conducting audits and carrying out cybersecurity risk assessments" (Allen & Gledhill, 2018). The CII owners now have to provide technical information relating to CII and are made to set up threat detection measures whilst adhering to strict standards and codes (Ang, 2018). Now, with this set of duties clearly laid out in front of them, they will be much more capable of working toward preventing cybersecurity breaches because the Cyber Security Agency gives directions to organisations providing critical services, on specific security measures they have to adopt (Baharudin, 2018).

Finally, CSA does assist the law in one regard. It officially criminalised circumvention of technological access control applied to copyrighted work, under section 261C (Kok & Cheang, n.d.). This means in previous years, the act of revealing data controllers had never been explicitly clear in legal terms, which made it difficult for authorities to charge perpetrators for. As hinted by Gasser (2006), with the presence of CSA, there is strong deterrence for individuals and businesses supplying technological mechanisms that seek to transfer data to a beneficiary without official permitted use or illegal "reproduction of computer programs for the purpose of interoperability" (p.54).

Evidently, this law has brought about a plethora of enhancements and adjustments that will serve to benefit Singapore in the long-run regardless of the situation of the current industry. However, were there any previous or existing laws around that were adequate enough to handle such cybersecurity 'gaps' that were clearly present in the country? The essay now shifts focus toward this juncture.

Are there no previous laws, or existing laws that are capable of handling CSA 2018?

Prior to this, there was no such thing as a '3-year' re-evaluation exercise required for CII. What this means is that, before the enactment, there may have been aspects of CII that changed (i.e, business, industry, clientele) without any proper re-evaluation of security measures. Now, the CSA ensures that CII undergoes timely evaluations to ensure their status as a functional and robust CII that is more resistant to attacks (CSA IFAQ, 2018)

Previous laws have actually given room for people who trade in illegally obtained personal information to not be formally charged. Now, with CSA, they can be formally charged with an offence even if they did not perform the hacking themselves (Hio, 2017). As of Jun 2020, there has yet to be a conviction specifically pertaining to this particular charge, but the act has enabled this to be an additional presence of enforced law.

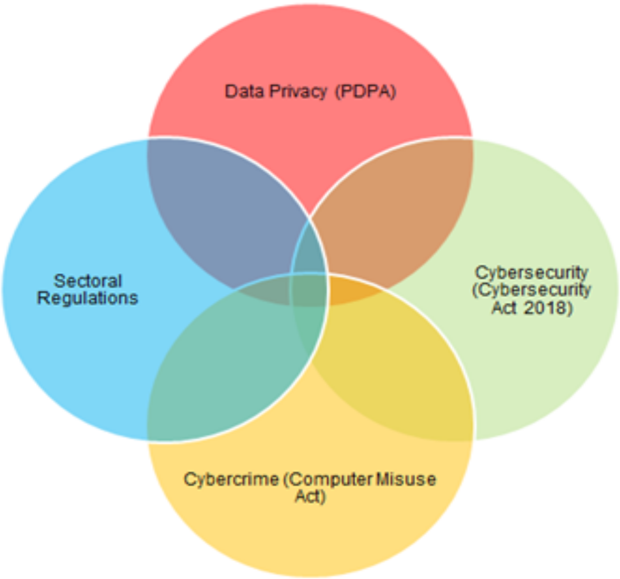
The 2017 Computer Misuse and Cybersecurity (Amendment) Bill criminalises the act of dealing and trading in personal information but does not explicitly charge those who sell the tools (Hio, 2017). Only after the CSA's enactment in 2018 did buying and selling hacking tools for illegal activities become recognized as a crime (Hio, 2017).

In 2012, the PDPA act (Personal Data Protection Act) was launched to establish a regime of data protection but it did not provide clarity on reasonable security arrangements that can be adopted by organisations which handles valuable personal data (such as, but not limited to, Data Breach Guide, Securing Personal Data Guide). Only with the enactment of CSA did such arrangements become clearer (Kok & Cheang, n.d.).

Beyond the CSA, MCI also stated they intend to explore implementing administrative arrangements and partnerships to facilitate and encourage information sharing; the importance of this dynamic is that it shows that there is insufficient productive yet safe information sharing, discussions and partnerships, between cybersecurity organizations, prior to the implementation of CSA (Kok & Cheang, n.d.).

Before CSA, there was actually the presence of a mutual gap that the PDPA, Sectoral regulations and CMA all had (see Figure 1 below). CSA successfully filled up in terms of contending with managing cyber risks and securing a stronger cybercrime legal framework.

Figure 1:


Data Privacy (PDPA)
Sectoral Regulations
Cybersecurity (Cybersecurity Act 2018)
Cybercrime (Computer Misuse Act)

Singapore's cybersecurity legal framework with multiple legislations
(Cramer et al., 2018)

Without the presence of the CSA, the PDPA, Sectoral regulations and CMA would not have been nearly enough in order for Singapore to bolster their cybersecurity resilience on her journey to become a smart nation. This implementation of the act was not just encouraged and recommended, it is necessary (Cramer et al., 2018).

With all this being said, we have to proceed with caution because there are several areas of consideration we must take into account in order to not get complacent or blindsided into thinking that this act is flawless and comes without natural cons.

Concerns about usage of the Cybersecurity Act

The act mainly revolves around how the commissioner chooses to utilize its broad powers under the CSA in requiring CII owners to furnish information related to CII. Potentially, there is a risk here due to the paradigm of power. To let this amount of power fall into the hands of a single entity could lead to unnecessary or reckless cybersecurity risk assessments and audits when inspecting companies complying with CII with standards of performance and CSA. However, there is no evidence to suggest this at the moment. Also, there may be a clash of sectors when it comes to disseminating responsibilities and powers related to cybersecurity; this concern in particular, while being slightly valid, has not yet surfaced in a real-life mishap yet.

The implementation of more cybersecurity obligations imposed onto CII will impose financial burdens on companies and, in an implicit long-term effect, chain supply relations may be affected as well. Relations in other areas can also be of a risk because, due to the licensing of certain cybersecurity services, it may lead to customers being more selective as to which cybersecurity vendors they choose to engage with. While there have not been any published examples of financial burdens imposed at this moment in time, it is important to be aware of these concerns as they can be detrimental to the reputation of the CSA.

Real life case studies of concerns

Firstly, it can be difficult for companies to find resources to maintain their cybersecurity strength of protection whilst managing other parts of that particular business; for instance, on 21 Apr 2016, PDPC imposed financial penalties of 36,800USD and 7370USD on ‘K Box entertainment group’ and its data intermediary, Finantech Holdings, for failing to implement proper and adequate protective measures to secure its system which led to 317,000 K Box members personal data being leaked on a public site. The CSA may actually lead to, potentially, businesses without the proper expertise or management to handle cybersecurity threats, to lose a lot of resources without sufficient notice (Ting and Lim, n.d.).

In another instance, for delegating responsibilities, the assistant cyber commissioner would “likely be an officer from the Monetary Authority of Singapore”; this is done in order to cut down the burden on CII owners (Cramer et al.m 2018) but simultaneously, there is a chance that a lack of awareness or knowledge from the financial officer to deal with the cyber side of things can create a miscommunication if not dealt with meticulously.

From a business point of view, CII owners will be heavily impacted as the obligations will result in increased costs due to having to keep up with all of the new cybersecurity measures of CSA (Cramer et al., 2018). From an organisation's perspective, since they are involved in the technology supply chain, CII owners would seek to impose contractual obligations on partners in order for full communal and mutual compliance with the act but this can result in an increase of costs incurred (Cramer et al., 2018).

With everything covered so far, we will now shift the essay into a direction that critiques the overall effectiveness of the act.

How has it been used and its effectiveness

Till date, the CSA has been used to penalise any person who fails to comply with the Commissioner's notice in providing information. The penalty is up to SG$20,000, imprisonment of up to 12 months or both (CSA 2018, pp.58). The CII organisations may also be subjected to regulatory actions, remedial measures and investigations by the Commissioner, as a result of non-compliance with the CSA. In another instance, the CSA is used for similar penalties for cybersecurity service providers that fail to adhere to the licensing regime. The service providers could be liable for "a fine of up to SG$10,000, imprisonment of up to 12 months or both" (Kok & Cheang, n.d).

The CSA has a framework for information request, data protection and sharing of the information. Moreover, the CSA facilitates information sharing which is vital in giving timely data for the government and owners of computer systems to detect vulnerabilities and deter cyber-attacks effectively (Cyber Security Agency of Singapore, n.d).

There is responsibility for CII owners to report specific cybersecurity incidents to the new cybersecurity commissioner and reveal CII data to the commissioner, which includes the design, security configuration of the infrastructure under the CSA framework. The CII owners have to "undergo periodic cybersecurity audits and risk assessments", which are required for adherence to codes of practice (Tan, 2018, pp 1). Additionally, they have to be involved in "cybersecurity testing exercises" as part of this new act. (Tan, 2018, pp 1).

Pandemic time

Singapore too, has seen herself fall victim over the covid pandemic to a flurry of cyberattacks. In the Asia-Pacific alone, Singapore has "made the largest shift" (Shiying, 2020) in the transition to work from home. The attacks comprised of "connections to malicious sites on the Internet" and "phishing attacks" (Shiying, 2020). Cyber-attackers are not fooling by any means, and it shows in how timely they seized a great opportunity by "taking advantage of the influx in potential victims" (Khandelwal, 2020). Looking at just the first half of 2020, when the virus and the shift to a new working environment/lifestyle was still something people were getting adjusted to, Singaporeans were "cheated of $82 million" which is "double the amount" that of 2019 (Khandelwal, 2020). Their adaption to consumer behaviour has seen them increase their use of sophisticated tactics, disguise schemes and impersonation ploys (Khandelwal, 2020). This worryingly begs the question as to whether Singaporeans are sufficiently "digitally literate", which could have a ripple effect on the efforts made by Singapore's response measures to the rise of cyberattacks.

One big step in the right direction, is a new programme titled "CII Supply Chain Programme", which is currently undergoing development by the Cyber Security Agency (CSA) of Singapore, via engaging CII owners and external consultants. (Chee, 2021). The programme helps cover owners of CII and vendors in 11 sectors (Government, Security, Healthcare, Media, Finance, Energy, Water, Infocomm, Maritime, Aviation and Land Transport) and will help to recommend processes and sound practices for all stakeholders to manage cybersecurity risks in the supply chain. (Chee, 2021). The introduction of such a comprehensive response measure is a great addition to Singapore's current state where the mindset related to cybersecurity risks must be spearheaded by industry leaders; as per Loh, "business leaders need to show their commitment to cybersecurity" (2019). What better way to show commitment than devoting efforts to a nationwide programme that covers most of the vital sectors in Singapore, and benefits stakeholders in a counter-measure effort to cease the rise of cyberattacks in the country? Speaking of which, these stakeholders would also be involved in discussions with the government in collective efforts to improve policies around the supply chain security (Chee, 2021), so all in all it does look like a win-win for all involved, only time will tell. If the country continues to keep a flexible and adaptive mindset, as they have shown via the creation of this programme, there is great hope that they will be able to combat the cyber attackers for the foreseeable future and beyond.

Cybersecurity Policy in Indonesia

The lack of legislation and cyber security awareness in Indonesia may bring some problems (Paterson, 2019). Certain cyber incidents, such as data breaches and massive electricity blackouts in Java in Aug 2019, demonstrate how important cyber security policies are for the nation. With how empowering technology is nowadays, selecting cyber security providers for the critical infrastructure and ensuring cyber security compliance is integral in order for the cyber security law in Indonesia to be effective. Moreover, Indonesia needs to establish a cyber security culture that goes beyond improving technological defences, but also require the peoples' resilience in this regard (Ulum, 2017). Technological solutions, such as investigating risk management aspects of security ranging from assessment of threat, vulnerability, cryptography, penetration testing, firewall, cloudflare etc, should be actively considered. With that being said, cyber security literacy and education need to be implemented from the onset, such as the usage of WIFI network, Virtual Private Network (VPS), updating anti-virus software, awareness from social engineering, changing passwords regularly, etc. These activities must be encouraged through the empowerment of cyber security culture.

The reason behind enacting cyber security measures

The Indonesian government sought to establish the Crypto and Cyber Security Agency (BSSN) in the beginning of 2017. The reason for this institution was due to the increase of counter-cyber terrorism incidents, escalation of fake news, and the desire to strengthen support for the digital economy in Indonesia. Indonesian digital start-up companies are already burgeoning and need to be supported by the appropriate cybersecurity policy (Kompas, 2017).

Some programs are conducted by the BSSN such as the establishment of honeynet project which shows the cyber-attack trend, develops security advisories based on CVE, provides the Voluntary Vulnerability Disclosure Program (VVDP) and encourages a standard for cyber security professionals. On 1 Aug 2020, for instance, the BSSN honeynet delianates the malware inclination attacked Indonesia (such as Malware Win.32.Generic.C.1960796, Trojan WIn 32.Swisyn.C2.105126, etc.) and according to the honeynet monitoring website, Indonesia is the most severely hit as it obtains 4.426.412 cyber-attacks whilst in comparison, India suffered 3.796.012 cyber-attacks and Vietnam received 2.763.470 cyber-attacks. Indonesia is the most badly hit country in this regard.

In order to strengthen the cyber security system, Indonesia needs such a regulation to cover the whole part of protecting critical infrastructure and safeguarding the cyber security ecosystem in Indonesia. The Presidential Regulation Number 53 of 2017, which was already amended to Presidential Regulation Number 133 of 2017 concerning the establishment of the Indonesia Cyber and Crypto Agency (BSSN), stipulates the responsibilities of the government in working towards enhancing cyber security. The BSSN has the authority to create, implement, oversee, and evaluate a technical policy in the area of identification, detection, and protection of e-commerce, crypto policy, cyber diplomacy, crisis management, information centre, education, coordination, from cyber incidents, cyber-attacks, etc. (Article 3 of the Presidential Regulation No. 53/ 133 of 2017). At present time, the BSSN creates cyber security alerts and allows public white hackers to list and report incidents through the Voluntary

Vulnerability Disclosure Program (VVDP).

In terms of cybersecurity management, the Indonesian government works with multiple stakeholders. The initiation, authority and responsibility for cybersecurity rests not only with the BSSN, but also with the Indonesian Ministry of Defence, Ministry of ICT, National Intelligence Agency and Indonesian National Police, just to list a few.

Beside these government institutions which have responsibility and tasks to develop cyber security, the Ministry of ICT also established the Indonesia-Security Incident Responses Team on Internet Infrastructure (ID-SIRTII), which officially began in 2006. This institution contains legal experts and digital technology experts who work together to strengthen the cyber security system in Indonesia. This institution was established by the Ministry of ICT Regulation No. 27/ PER/ M. Kominfo/ 9/ 2006 and revised in No. 26/ Per/ M. Kominfo/ 5/ 2007 concerning the telecommunication network security-based internet protocol. This institution monitored connectivity transaction records such as log files, ports, cyber-attack detection and early warning systems.

Other regulations that support cybersecurity

Indonesia only has two regulations which support their cyberspace ecosystem, namely; Telecommunication Act No. 36 of 1999 and the Electronic Information and Transactions (Undang-Undang Informasi dan Transaksi Elektronik, UU-ITE hereinafter also referred to as 'Indonesia ICT Law), Law No. 11 of 2008 which was later on revised into Law No. 19 of 2016. The Indonesia ICT Law is often used as a legal basis for the digital technology environment. Despite the Indonesia ICT Law's original purpose of regulating and protecting electronic business transactions, at the present time it can also be used to regulate cyberspace (Lim, 2013).

The Indonesia ICT Law may cover various cyber incidents. In Indonesia, the cyber incidents can be recognised through a variety of scopes such as computer virus, data leakage, carding, cracking, hacking, illegal access, Trojan Horse, infringement of intellectual property rights, illegal interception, online pornography and many others (Siburian, 2016). Most cases are reported to the Indonesian National Police which mainly consist of computer-related forgery and fraud or phishing related incidents (Bunga, 2019). Furthermore, the investigation of cyber incidents in Indonesia may also tap into considering digital evidence held by the Forensic Laboratories of the Indonesia National Police (Prayudi, 2015)

In 2008, after the issuance of the Indonesia ICT Law, cyber incident investigation and enforcement became popular. However, cybercrime has been prevalent since decades ago. In 2001, there was an e-banking fraud within Bank Central Asia (BCA). Furthermore, in 2004 the pseudo-name of Xnuxer conducted defacement activities and edited the names and pictures of political parties (M Irfan, MA Ramdhani, 2018). Over the past five years, cyber incidents in Indonesia are mostly composed of cases of fraud, phishing and illegal access.

Focus Cybersecurity Policy

In the near future, the Indonesian Government should prepare the cyber security bill to regulate the cyber security ecosystem. If the bill is passed in parliament, the value of multi-stakeholders' effort will be taken into consideration. It is not just the BSSN that plays a significant role, but also the Military Forces, Intelligence Affairs, Ministry of ICT, Indonesian National Police and many other government institutions. Besides the government bodies, the cyber security ecosystem is also constructed by universities and communities. Some universities have opened special programs on cyber security such as the Binus University, Bandung Technology Institute and Telkom University, to name a few. Various communities and associations also established cyber security ecosystems alongside universities and government bodies in Indonesia. There are also some communities and associations which actively align to entities such as the Indonesian Internet Service Provider (APJII), Indonesian Cyber Security Forum (ICSF) and Indonesia Association for Digital Forensic (AFPI). These communities frequently provide meaningful insights to the government and help to conduct conferences and seminars, which create good networking opportunities

Indeed, digital connectivity in Indonesia creates a plethora of economic opportunities, but it also brings about several problems in the form of cybercrime, cyber-attack, and moreover, cyber-amplified religious intolerance and disinformation (Paterson, 2019). The economic opportunities present within digital connectivity in Indonesia is very promising. In 2018, Indonesia received 27 trillion USD from the digital economy and this figure is set to bloom toward 100 trillion USD in 2025 (Temasek and Google, 2018). Furthermore, since 2015, Indonesia gained an approximate of $ 409 million USD annually and that figure will increase over time (Hedrich et al., 2017). However, digital economy also presents a lot of risks in regards to piracy of works, plagiarism, illegal downloading (software, film, music etc.), illegal content (pornography), hoax, sexual harassment and the transaction of dangerous goods (drugs, weapons, bombs, etc.) which is scattered all over the internet (Fahlevi et al., 2019). At the same time, the lack of knowledge about cyber security culture in society is in itself altogether, another heavy problem (Ulum, 2017).

Indonesia's promising potential of their digital economy is existent through the growth of digital platforms, especially successful examples of Gojek and Tokopedia (Paterson, 2019). The Indonesian Government has already started to improve cyber security systems by enhancing technical and procedural measures that have already been undergoing developmental progress, such as the establishment of Indonesia National Standard (SNI ISO/ IEC 27001/ 2009 concerning Information Security Management System), the installation of health and safe internet system with creating the Trust +: Trust Positive; which filters domains, URLs, Content, Keywords and Expressions (Setiadi et al., 2012). In the near future, the Indonesia government definitely needs more regulations in order to safeguard the cyberspace landscape. Regulations such as the Cyber Security Act, Data Protection Act, Interception Act and Social Media Act, have really demanded for the ecosystem of cybersecurity and digital economy in Indonesia to be strengthened and bolstered.

Some cases related to cyber incidents

Some cases that have occurred in Indonesia concerning data breach and cyber incidents shows and proves that indeed, there is no system equipped to be bullet proof from cyber-attacks. Private and Public institutions in Indonesia, along with many individuals, have suffered from cyber-attacks and data breaches. Hence, the Indonesian cyber ecosystem requires a strong approach and strategy to build an adequate response of capable prevention from cyber incidents

In March 2020, one of the largest e-commerce businesses in Indonesia, Tokopedia, suffered a data breach resulting in 15 million users' data being compromised (Kompas, 2020). Shortly after that, Twitter Account named "@Underthebreach" announced that the personal data of 91 million users had already been sold on the dark web for a sum of $ 5000 USD (Faradifta, 2020). Personal details such as full name, email, address, place and date of birth, latest login, mobile number, and other important private data were stolen (Kompas 2020). Tokopedia responded by reminding users to change their password regularly and proceeded with conducting a full investigation. They also reported to the Ministry of ICT whilst coordinating with the Indonesian Crypto and Cyber Agency (BSSN), and sought assistance from the Indonesian National Police. However, it seems that further investigation for this data breach was not proportionally described to the public.

David Tobing, a lawyer who represented some Tokopedia users, filed a lawsuit through civil law procedure against this e-commerce company (Kompas, 12/ 06/ 2020). This appeal is related to Article 26 of ICT Law which mentioned that in any damage from data breach, the data subject may sue the company. The case was handled by the Central Jakarta Court.

The Tokopedia saga was not the only case; In 2017, Bukalapak was also reported to be suffering from data breach and the latest case happened to Bhineka.com. Besides private companies, public institutions such as the Indonesian General Election Commission (KPU) also experienced a data breach. This case was announced by Teguh Aprianto, the head of Indonesian Ethical Hacker Community, on his Twitter account. A List of approximately 23 million voters (which was provided by the KPU) was already sold in a dark website (Parama, 2020). He claimed that the data breach caused a wide list of personal data (full name, identity number, place and date of birth, age, gender, marital status, and address) to surface on the dark web. However, at the same time, the KPU insisted that there was no data breach and they stated the list of voters stemmed from previous data recorded in 2014 (Kompas, 2020)

If the perpetrator is prosecuted, he or she may face charges for illegal access (Article 30 of ICT Law) and data theft (Article 32 of ICT Law). Those found guilty of Illegal access can be punished for 6 (six) years or a fine of 600 million IDR (according with $ 60.000) in accordance with Article 30 of ICT Law. Meanwhile, data theft offenders can be charged for 8 (eight) years or fined a sum of 2 billion IDR (accordance with $ 200.000).

Effectiveness of cybersecurity policy in Indonesia

Due to the absence of a cybersecurity act, the effectiveness of cybersecurity policy in Indonesia is inadequate. The only specific regulation concerning cybersecurity is the Presidential Regulation on the establishment of the BSSN. Additionally, the Indonesian government has several regulations related to cybersecurity such as the Law of Indonesian National Police, State Defence, Counter-terrorism, National Armed Forces, and ICT Law (Rizal&Yani: 2016); yet, the existence of a national cybersecurity act is very much needed. This potential nationwide regulation of cyber security may enhance the digital ecosystem with stronger political will, strengthen budgeting support, escalate governmental responsibility, and the increased usage of criminal provision to enforce the law strictly.

Moreover, a cybersecurity act could help encourage Indonesian people to establish a resilient cybersecurity culture. The citizens can apply cybersecurity measures in securing their information and be trained to take appropriate steps once faced with potential cyber threats (Ulum: 2017). They can also take reference from the National Police Report concerning cybercrime rate as many cases contain online fraud and these cases may be due to the unawareness of members in society to safeguard their electrical belongings and secret information.

However, combating cybercrime can be implemented through the existing telecommunication law and ICT Law. Until 2020, the case law related to cybercrime is already published in the supreme court website which contains over 1,300 cases. Some of them had already proceeded with computer crime and computer related crime. This means the work of combating cybercrime in Indonesia is also the same as the strengthening cybersecurity ecosystem.

Cybersecurity in the era of pandemic time

Some cyber incident cases happened during the COVID-19 pandemic. It has occurred at some e-commerce businesses along with public online applications; all of which have suffered from some form of data breach. Furthermore, there are significantly more people working from home and using the internet for daily activities. On April 10, 2020, The Indonesia Crypto and Cyber Security Agency released a security alert for using video conferences. They announced that video conference applications can be hacked by cybercriminals whilst people are using the internet to work from home. The government warned people to stay at home during the pandemic era to stop the infection and highly encouraged working from home as well as implementing the closure of some offices. However, the aforementioned challenges were reported by some publications by Indonesia Crypto and Cyber Agency related to cyber-attack on video conferences.

To prevent the escalation and infection of COVID-19 Virus, the Indonesian government persuaded people to practice social distancing and physical distancing plus encouraged them to conduct work from home (WFH). Some critical infrastructures related to the treatment of COVID-19, which involves and deals with health and safety, have been required to operate during this difficult time in spite of the pandemic

Since January 2020, there has been an increase of people falling victim to an increase of cyber-attacks by cybercriminals who have been using the pandemic to take advantage of some difficult situations people have found themselves in, unfortunately. These cybercriminals are using some techniques to target the victims.

For instance, cybercriminals created fake emails (phishing) to look like they were related to COVID-19 issues but in reality, exploited users by sending malware such as AZORult, Cerberus, Lokibot and Trickbot. They used platforms such as email, instant message and fake websites to appear as if they were "COVID-19 related". Another technique was that they claimed to be representing authority figures in handling COVID-19 Virus and falsely informed the victims that they were WHO staff or government agency staff working to prevent the further spread of COVID-19 Virus and so on and so forth. Therefore, Indonesia Crypto and Cyber Security Agency warned people to adopt critical thinking and to be alert when reading and using information concerning the virus, as there could be fake threats lying in wait

In response, the Indonesia Crypto and Cyber Security Agency suggested people to practice a degree of safety by using video conference applications with some preparations. For example, they should be updating the video conference application regularly or ensure they are using the current version of the application. Other suggestions included the usage of VPN, enabling encryption, limiting the usage of share screen and to frequently use complex passwords. During the pandemic, cyber-attacks happened four times the amount than at the end of 2020 (Kompas, 12/10/20); regretfully, it will possibly be continuing when people are still working from home and often use the internet.

Similarities and Differences Between Indonesia and Singapore

This section will compare the legal system between Indonesia and Singapore. The similarities and differences both countries have been obtained from literature review. Starting with similarities, both countries have a strong commitment to enhance cybersecurity. Both countries have their own regulations concerning cybersecurity and have ad hoc institutions dealing with cybersecurity issues. For instance, the Indonesian Crypto and Cyber Agency (BSSN) in Indonesia and Cyber Security Agency in Singapore are examples of ad hoc institutions responsible for enhancing the cybersecurity ecosystem.

The role of cybersecurity agencies in both Indonesia and Singapore have important measures in enhancing national cybersecurity systems and culture. Both agencies encourage the quality and consistency of improving penetration testing, managed security operation centre, investigating the cyber incidents, etc. The national and international cooperation in the field of cybersecurity is also a pivotal part of these agencies' role. The Indonesian Crypto and Cyber Agency (BSSN) in Indonesia and Cyber Security Agency in Singapore also conduct research and development to support cybersecurity technology and human resources. Overall, these institutions have the following responsibilities to promote the cybersecurity, advice the Government and public authorities, monitor cyber threats, investigate cyber incidents that damaging national security, defence, economy, public health, public order or public safety, etc, cooperate with national or international computer emergency response teams (CERTs), etc. For the most part of their functions, these institutions, the Indonesian Crypto and Cyber Agency (BSSN) in Indonesia and Cyber Security Agency in Singapore, look similar

Both countries also face cybersecurity threats. First, the growing of the digital economy in both countries will give an opportunity to encourage digital start-up and e-business in upgrading cybersecurity awareness. Second, the cyber threats such as phishing, business email compromise, spam, malware, DDoS, defacement, ransomware, remote access trojan, and other cyber threats until cyber-terrorism may accompany the development of digital economy ecosystem. Indonesia and Singapore have a close relationship as neighbouring countries and partners throughout ASEAN region. They have collaborated on a program concerning cybersecurity. Indonesian Minister of Legal, Political and Security Affairs Wiranto had attended 'the Singaporean International Cyber Week 2017' (Straitstimes: 2017).

As it can be seen that the cybersecurity threats encompassed the world. No county is immune from cyber-attack and data breach. However, we have to fight to strengthen cybersecurity in reducing more potential harm from cyber-attacks. Indonesia and Singapore have also witnessed some cases related to data breach. For instance, as mentioned in the sections above, millions of Indonesian voters have breached their personal data such as identity number, full name, address, etc from the hacking case which suffered the Indonesian Commission Election. As discussed above, Singapore has also had cases of data breach such as the Singhealth IT systems which were attacked and exploited by cyber criminals. Both countries have similar cases of data breach which should enhance cybersecurity policy, system and culture over time.

After we discuss the similarities between both countries, we will investigate the differences. Singapore has the CSA which is a product from legislation. This means that the legal binding power effect is stronger which equipped with criminal provision for non-compliance. Whilst, Indonesia still struggles to develop the cybersecurity bill which needs to be made possible by the Indonesian Parliament in 2021

Furthermore, the CSA being legislated, suggests a stronger legal muscle given to Cybersecurity Agency. At the same time, the Indonesian Crypto and Cyber Agency (BSSN) was established by the Presidential Decree in 2017. The function of BSSN plays an important role in enhancing the cybersecurity system in Indonesia. However, the multi-stakeholder's approach could be another alternative to attract more participants from state institutions to handle cybersecurity issues in a broader aspect.

The CSA seems to focus on safeguarding the critical infrastructure. Part 3 of CSA stipulates the legal norm concerning CII ranging from design, codes of practice and standards, audits and risk assessments, etc. Meanwhile, Indonesia cyber security policy tries to cover all cyberspace not only critical infrastructure, but also digital economy, public services, digital creative industries, cybercrime, etc.

In Singapore, punishments are incorporated in CSA. For instance, providing cybersecurity service without licence will be convicted for $ 50.000 or imprisonment for 2 years, failed to comply commission's notice will be convicted for $ 100.000 or imprisonment for 2 years, failed to furnish information relating to critical information infrastructure for owner with fine sum of $ 50.000 or imprisonment for 2 years, and so forth and so on. Whilst, Indonesia cybersecurity policy cannot provide the criminal provision since it has not been enacted as a national regulation or a product of legislation. If any cyber incidents are connected to cybersecurity problems, the Indonesia ICT Law and Telecommunication Law may be triggered.

Last but not least, as we can see that there are differences and similarities between Indonesia and Singapore. Both countries have a special task for their respective cybersecurity agencies which takes on the responsibility for deterring cyber incidents, securing national cyber space, and so on. Furthermore, both countries realised the cyber-attacks and threats as a challenge to improve the cybersecurity system and culture. At the same time, Singapore is more focused on securing critical infrastructure while Indonesia tries to cover broader scope such as overseeing the digital economy. Furthermore, in Singapore, cybersecurity has already become the act of regulation, which stipulates the criminal provision for the infringement of this act. Whilst, cybersecurity regulation bill is still on the legislative-making process, the present time, the Presidential Regulation and ICT Law become a legal ground.

Conclusion

The commitment of strengthening cyber security ecosystem is very important to combat cybercrime and safeguard data security in the critical infrastructure sector. The description above mentioned the cyber security policy in Singapore and Indonesia, which delineating the role of cyber security agency and the cyber security policy is a pivotal component. Cyber security can investigate cyber incident which involved many victims and sensitive data. For instance, in June 2018, as mentioned above, hackers breached the 1.5 million patient's data of the SingHealth IT systems. In Indonesia, it was happened the data breach involved the voter data of general election, then the Indonesia Cyber and Crypto Agency had involved in the investigation. Despite, the agency had failed to arrest the cyber criminals, the prevention and reparation of IT security system in the critical infrastructure and public electronical good is very important. During the pandemic, people use the internet more and need to be secured.

This article discussed the similarity and differences of cyber security policy in Indonesia and Singapore. Both countries have a special task agency to handle the issue of cyber security. In Singapore, the Cyber Security Agency plays a significant rule as well as the Indonesian Crypto and Cyber Security Agency in Indonesia. As the regulator in the field of cyber security, these institutions have responsibility to investigate cyber incidents, safeguard the critical infrastructure, and enhancing the cybersecurity ecosystem in both countries. These institutions have a rule to make an international cooperation in the field of cyber security. Furthermore, both countries have a regulation concerning cyber security such as Cyber Security Act of 2018 in Singapore and the Presidential Regulation Number 53/ 133 of 2017 concerning the establishment of the Indonesia Cyber and Crypto Agency.

Beside the similarities, cyber security policy in Indonesia and Singapore can be seen from some differences. From regulation, in Singapore, Cyber Security focuses on the issue of safeguarding critical infrastructure and the form of law issued by the Act of Parliament. Furthermore, cyber security regulation issued by the Presidential Decree in Indonesia. However, the area of cyber security authority is not only the protecting critical infrastructure, but also identification, detection, enforcement, monitoring, crypto, cyber diplomacy, crisis management, e-commerce, and many other things related to cyber security.***

Bibliography

Ang, B (2018) Singapore Cybersecurity Strategy And Legislation (2018). [online] Slideshare.net. Available at: <https://www.slideshare.net/benjaminang/singapore-cybersecurity-strategy-and-legislation-2018> [Accessed 10 June 2020].

Allen & Gledhill (2018) Singapore. [online] Allen & Gledhill. Available at: <https://www.allenandgledhill.com/sg/publication/articles/7545/cybersecurity-act-2018-operative-from-31-august-2018-to-protect-critical-information-infrastructure-against-cybersecurity-threats> [Accessed 10 June 2020].

Angkasa (2018) Legal Protection for Cyber Crime Victims on Victimological Perspective. SHS Web Conf. 54 08004, 1–6.

Bunga, D (2019) Legal Response to Cybercrime in Global and National Dimensions Respon Hukum terhadap Kejahatan di Dunia Maya dalam Dimensi Global dan Nasional A . Introduction Cybercrime is a crime phenomenon in the era of digitalization that threatens global security an. Padjajaran J. Law 6, 69–89.

Chan, Francais, (2017) Indonesia and Singapore to cooperate on cyber security: Wiranto, https://www.straitstimes.com/asia/se-asia/indonesia-and-singapore-to-cooperate-on-cyber-security-wiranto

Chee, K (2021) Push to better manage cyber-security risks in critical infrastructure. [online] The Straits Times. Available at:

<https://www.straitstimes.com/singapore/push-to-better-manage-cyber-security-risks-in-critical-infrastructure> [Accessed 8 March 2021].

Chua, A (2017) Mindef Hit By Targeted Cyber Attack. [online] TODAYonline. Available at: <https://www.todayonline.com/singapore/mindef-internet-system-hacked-personal-data-850-personnel-stolen> [Accessed 10 June 2020].

Cramer, S., Ang, W., Olds, D., Paulin, J. and Lua, J (2018) Singapore's New Cybersecurity Act Comes Into Force: Here's What You Need To Know | Data Protection Report. [online] Data Protection Report. Available at: <https://www.dataprotectionreport.com/2018/09/singapores-new-cybersecurity-act-come-into-force-heres-what-you-need-to-know/> [Accessed 10 June 2020].

CSA, 2018. Cybersecurity Act. [online] CSA Singapore. Available at: <https://www.csa.gov.sg/legislation/cybersecurity-act> [Accessed 10 June 2020].

CSA IFAQ, 2018. FAQ. [online] Cyber Security Agency. Available at: <https://www.ifaq.gov.sg/csa/apps/fcd_faqmain.aspx#FAQ_2109835> [Accessed 10 June 2020].

CSA. n.d. [online] Available at:https://www.csa.gov.sg/legislation/cybersecurity-act#:~:text=Establish%20a%20framework%20for%20sharing,prevent%20cyber%20incidents%20more%20effectively [Accessed 9 June 2020].

Erdianto, Kristian (2017) Alasan Pemerintah Mempercepat Pembentukan Badan Siber Nasional. https://nasional.kompas.com/read/2017/01/03/21285241/alasan.pemerintah.mempercepat.pembentukan.badan.siber.nasional?page=all, accessed on June 30, 2020

Faradifta, Chintiara (2020) Tanggung-jawab Hukum Penyelenggara Sistem Elektronik atas Data Pribadi Pengguna Sistem Elektronik terhadap Pihak Ketiga dalam Perspektif Pemidanaan. Universitas Bhayangkara.

Fahlevi, M., Saparudin, M., Maemunah, S., Irma, D., Ekhsan, M (2019) Cybercrime Business Digital in Indonesia. E3S Web Conf. 125, 1–5. https://doi.org/10.1051/e3sconf/201912521001

Hedrich, W., Wong, G., Yeo, J (2017) Cyber Risk in Asia-Pacific The Case for Greater Transparency. Marsg&McLennan Companies, Inc.

Hio, L (2017) Laws Changed To Keep Pace As Cybercrime Evolves. [online] The Straits Times. Available at: <https://www.straitstimes.com/singapore/laws-changed-to-keep-pace-as-cybercrime-evolves> [Accessed 10 June 2020].

Kaspersky (2020) Hacking the pandemic: new documentary reveals healthcare cybercrime surge amid COVID-19, https://www.kaspersky.com/about/press-releases/2020_hacking-the-pandemic, accessed on February 15, 2021

Khandelwal, S (2020) Commentary: The year hackers and scammers exploited our COVID-19 fears to cheat us. [online] CNA. Available at:

<https://www.channelnewsasia.com/news/commentary/covid-19-cybersecurity-phishing-scam-crime-hack-online-protect-13635524> [Accessed 8 March 2021].

Kok, A. and Cheang, K., (n.d). Added Security Comes At A Price: The Impact Of Singapore's Cybersecurity Act | Lexology. [online] Lexology.com. Available at: https://www.lexology.com/library/detail.aspx?g=bf739778-4a49-4a95-8781-d79b9d429b75 [Accessed 9 June 2020].

KPMG (2019) What Is The Cybersecurity Act?. [online] KPMG. Available at: <https://home.kpmg/sg/en/home/insights/2019/03/what-is-the-cybersecurity-act.html> [Accessed 10 June 2020].

Loh, V (2019) The Big Read: As more cyberattacks loom, Singapore has a weak 'first line of defence'. [online] CNA. Available at: <https://www.channelnewsasia.com/news/cybersecurity-attacks-hacks-singapore-vulnerable-weak-first-line-11286586?cid=h3_referral_inarticlelinks_24082018_cna> [Accessed 8 March 2021].

Lim, M (2013) The Internet and Everyday Life in Indonesia : A New Moral Panic ? J. Humanit. Soc. Sci. Southeast Asia 169, 133–147.

M Irfan, MA Ramdhani, W.D (2018) Analyzes of cybercrime expansion in Indonesia and preventive actions. 3rd Annu. Appl. Sci. Eng. Conf. https://doi.org/10.1088/1757-899X/434/1/012257

Parama, Doly (2020) Tinjauan Hukum Perlindungan Data Pribadi di Indonesia. Universitas Bhayangkara.

Paterson, T (2019) Indonesian cyberspace expansion: a double-edged sword. J. Cyber Policy 4, 216–234. https://doi.org/10.1080/23738871.2019.1627476

Pertiwi, Wahyunanda (2020) Kasus Kebocoran Data Pribadi di Indonesia dan Nasib Perlindungan Data Pribadi.https://tekno.kompas.com/read/2020/05/05/19080067/kasus-kebocoran-data-di-indonesia-dan-nasib-uu-perlindungan-data-pribadi?page=2, accessed on June 30, 2020

Pertiwi, Wahyunanda (2020) Data 15 Juta Pengguna Diduga Bocor, Tokopedia Sebut Ada Upaya Pencurian. https://tekno.kompas.com/read/2020/05/02/22060847/data-15-juta-pengguna-diduga-bocor-tokopedia-sebut-ada-upaya-pencurian, accessed on June 30, 2020

Prayudi, Y., 2015. A Proposed Digital Forensics Business Model to Support Cybercrime Investigation in Indonesia 1–8. https://doi.org/10.5815/ijcnis.2015.11.01

Salsabila, Putri Z (2020) Kejahatan Siber di Indonesia Naik 4 Kali Lipat Selama Pandemi. https://tekno.kompas.com/read/2020/10/12/07020007/kejahatan-siber-di-indonesia-naik-4-kali-lipat-selama-pandemi, accessed on February 16, 2021

Shiying, W (2020) Cyber security threats on the rise as more people work from home: Cisco survey. [online] The Straits Times. Available at: <https://www.straitstimes.com/singapore/rise-in-cyber-security-threats-as-more-people-work-from-home-cisco-survey> [Accessed 8 March 2021].

Shiying, W (2020) Cyber security threats on the rise as more people work from home: Cisco survey. [online] The Straits Times. Available at: <https://www.straitstimes.com/singapore/rise-in-cyber-security-threats-as-more-people-work-from-home-cisco-survey> [Accessed 8 March 2021].

Setiadi, F., Sucahyo, Y.G., Hasibuan, Z.A., 2012. An Overview of the Development Indonesia National Cyber Security. Int. J. Inf. Technol. Comput. Sci. (IJITCS) 6, 106–114.

Shiying, W (2020) Cyber security threats on the rise as more people work from home: Cisco survey. [online] The Straits Times. Available at: <https://www.straitstimes.com/singapore/rise-in-cyber-security-threats-as-more-people-work-from-home-cisco-survey> [Accessed 8 March 2021].

Siburian, H.K., 2016. Emerging Issue in Cyber Crime: Case Study Cyber Crime in Indonesia. Int. J. Sci. Res. 5, 2013–2016. https://doi.org/10.21275/ART20162818

Tan, B (2018) [online] Pinsentmasons.com. Available at: <https://www.pinsentmasons.com/out-law/news/cyber-laws-take-effect-in-singapore> [Accessed 9 June 2020].

Tan, Zoe (2020) The state of cybersecurity in the time of COVID-19, https://usa.kaspersky.com/blog/cybersecurity-in-the-time-of-covid/22651/, accessed on February 15, 2021

Temasek and Google, 2018. e-Conomy SEA 2018.

Ting, S. and Lim, C., (n.d.) Cybersecurity In Singapore | Lexology. [online] Lexology.com. Available at: <https://www.lexology.com/library/detail.aspx?g=e8e0c6b8-d81a-4dfc-a8fe-36a1dd3baa54> [Accessed 10 June 2020].

Ulum, M., 2017. Cyber culture and cyber security policy of indonesia: combining cyber security civic discourse, tenets and copenhagen's securitization theory analysis. Proceeding 1st Int. Conf. Soc. Sci. Univ. Muhammadiyah Jakarta, Indones. 1–2 Novemb. 2017 Towar. Community, Environ. Sustain. Dev. 1–2.