Comparative Study of Cyber Security Policies among Malaysia, Australia, Indonesia: A Responsibility Perspective

Conference Paper · October 2015

DOI: 10.1109/CyberSec.2015.36

CITATIONS
2

READS
252

3 authors, including:

Arya Adhyaksa Waskita
Badan Tenaga Nuklir Nasional
7 PUBLICATIONS **10** CITATIONS

SEE PROFILE

Setiadi Yazid
University of Indonesia
23 PUBLICATIONS **99** CITATIONS

SEE PROFILE

Comparative Study Of Cyber Security Policies Among Malaysia, Australia, Indonesia: A Responsibility Perspective

P.D. Persadha[†*], A. A. Waskita[†‡], S. Yazid[†]

[*]Communication and Information Security Research Center,
Jalan Moh Kahfi I no.88D Jagakarsa Jakarta Selatan, Indonesia
Email : pratama@cissrec.org

[†]Faculty of Computer Science, Universitas Indonesia,
Kampus UI Depok, Depok 16424, Indonesia
Email : setiadi@cs.ui.ac.id

[‡]Center for Safety and Technology of Nuclear Reactor, National Nuclear Energy Agency,
Kawasan Puspiptek Serpong, Tangerang 15310, Indonesia
Email : adhyaksa@batan.go.id

***Abstract*—The significant growth of information and communication technology (ICT) has the potential to promote economic growth. On the other hand, it also cause an increase in cyber threat and hence must be handled properly. Comprehensive and collective approach in handling cyber threat should be considered as importance. One of the most important aspect that should be considered is organizational structures. It plays a significant role in organizing responsibility among cyber related agencies. This paper provides a comparison study about a delegation scheme of responsibilities in cyber related role among different agencies among three different countries Malaysia, Australia and Indonesia. This study has shown that Indonesia has a more complex partition scheme of delegating responsibilities.**

***Index Terms*—Cyber Security, Organizational Structure, Delegating Responsibilities**

I. Introduction

As the vast growing of information technology and internet development and deployment, it is much more easier for us to access information and knowledge. It is now easy for the information providers to communicate their product or policy to the users. A number of online applications such as e-commerce [1], media for disseminating teaching materials [2], and especially social media are growing rapidly in Indonesia. In fact, the amount of internet users in Indonesia is relatively large compared to internet users in the world [3].

Cyber threats that potentially disrupt the online services [4] up to financial losses, are also increasing [5]. MyCERT (Malaysia Computer Emergency Response Team) reported 4117 incidents for the first half of 2014 [6], where more than half are financially motivated, and a total of financial loss of AU$ 1.06 billion in Australia due to cyber crime [7]. Based on http://cybermap.kaspersky.com/, Indonesia ranks 7th as the highest cyber space infected country in early 2014. It will be more dangerous if a cyber threat is directed to a safety critical infrastructure [8]. Furthermore, a cyber crime is currently more organized, economically promising for the undeground community [9] and has became an everyday reality [10]. Its influence on the community in line with the growth of electronic information system that enables more online businesses [11].

Cyber security itself is a multidisciplinary and a multidimensional subject [12], [13], involving strategic, organization, policy, ethics, certification, law, technical, personnel and audit. Although many technical approaches to a cyber security have been developed, non-technical approach is nonetheless important to be considered. Even the greatest threat in information security, comes from carelessness of the internal users [14]. The development of cyber security should consider human behavior in designing, developing and implementation phase [15]. This is because humans are the weakest aspect in information security [16]. Consequently, information security culture cannot be separated from national and organizational culture where it is implemented [17]. In this paper, the term information security is used interchangeably with cyber security, although cyber security covers a wider aspect due to its additional aspects, namely the human as potential target of attacks [18].

Cyber security was defined as a collection of tools that can be used to protect cyber environment, organization, and user assets from cybercrime [19]. Therefore, it is es-

sential to create and implement an effective anti cybercrime strategy as part of national cyber security strategy. Based on ITU (International Telecommunication Union) anti cybercrime strategies, organizational structure is one of the most important strategies that should be considered. Comparing organizational structure among different nations with a number of similarities, e.g. culture, can provide a better understanding of how each country builds their anti cybercrime organizations. Thus, this paper compares about non-technical approaches regarding the development of cyber security between Indonesian government and few other nations, namely Australia and Malaysia. These two nations have a contradictory culture background whereas Indonesia is in between. Specifically, Indonesian culture has a close connection with Malaysia [20] but different from Australia [21], [22] which been dominated by western culture.

The paper is organized as following. After this introduction section, how the cyber security organizational structure of each nation is presented in Sec. II. Further, in Sec. III is where each organizational structure is discussed. To look at the efficiency of securing cyber environment, a hierarchy of responsibilities is evaluated. Finally, a conclusion is constructed as a suggestion to build efficient organizational structure of cyber security in Indonesia, especially related to the hierarchy of responsibility and authority of institutions.

II. Development of cyber security in different nations

A. Malaysia

As neighbors, Indonesia and Malaysia have a relatively similar culture. Likewise, Malaysia also exposed to cyber attacks, which lead to negative impact for them. One of the strategies that they have to overcome cyber threats is the law implementation regarding the matter [23]. Both Malaysian government and private organizations are involved to improve this approach.

From the government sector, a few institutions are responsible for handling cyber threats. One of them is the Ministry of Science, Technology and Innovation (MOSTI) [24] who is responsible for designing a framework regarding the national policy of ICT. Through this institution, Malaysia has developed a policy which been known as National Cyber Security Policy (NCSP) [25]. NCSP was born from the vision of Malaysia 2020 which stated that ICT is the key in every sector. For this matter, Malaysia has to accept the consequences of exposing their resources and information to cyber threats, especially if the cyber attack targets Critical National Information Infrastructure (CNII). Thus, NCSP is the real and thorough application to secure CNII. It is important to guarantee that CNII is safe, resilient and self reliant in order to increase national stability, prosperity and welfare.

CNII is integrated in every asset whether it is physical or virtual, system and function, that is important to the nation. So that any decrease in capacity or damage in it will jeopardized the national economy, image, security and defense, the ability of the government to work, and the public health and safety. From that definition, a few sectors could be identified as part of CNII, which are national security and defense, bank and finance, information and communication, energy, transportation, climate, health services, government, emergency services, food and agriculture [26]. Malaysia should be able to protect their CNII by implementing NCSP. Hopefully, national stability and prosperity can be increased.

To get technical support from NCSP, Cyber Security Malaysia (CSM) was made [27]. CSM has the responsibility to run services, which are Cyber Security Emergency Services, Security Quality Management Services, InfoSecurity Professional Development and Outreach and Cyber Security Strategic Engagement and Research. MOSTI is also used to supervise an agency respond to the computer emergency incident known as Malaysia Computer Emergency Respond Team (MyCERT) [6].

Malaysia also considers terrorist attack to the facility of CNII [28]. The tendency of terrorist attack through ICT is driven from the fact that it could have a major impact to the attacked nation, severe damage or suffer difficult conditions, due to cessation of essential services. For that matter, the use of ICT in terrorism is far more dangerous than conventional attack.

Another government institution that involved in implementing cyber security in Malaysia is The Malaysian Communications and Multimedia Commissions (MCMCs) [23]. This institution has the responsibility to monitor and regulate communication and multimedia activities in Malaysia. This includes regulation and supervision of telecommunication, broadcast, Internet Service Provider (ISP), postal and courier, and authority of digital certificate. MCMCs also has the power to shut down websites that have contents of blasphemy, pornography, fraud or incitement.

In additional to the two institutions above, there is also Royal Malaysian Police (RMP) with one of its department, the Department of Commercial Crime Investigation which also conduct Investigation of Cybercrime and Multimedia Unit [23]. Malaysia also built Computer Forensic Laboratory as a facility to train police officers and computer forensics.

B. Australia

Australia has implemented multiple policies to secure their cyber assets [29]. As cyber security is one of the most important policy for Australian government due to two reasons. First, it is important because of the impact that cyber attacks have on business and individual of Australia. Second, it is because of the potential disruption that cyber attacks give to the level of trust regarding Australian ICT as individual or as a group.

Cyber security has to be seen as a collective work. There is no organization that can handle every problem

on technology that can deal with every issue and meet all expectations [30]. Therefore, there are few different roles are created to handle cyber security in Australia [29]. The first role is the federal government of Australia, which has four responsibilities. First is to build, implement and enforce the law, rules and policies regarding cyber security. Then, it has to participate in global cyber security to improve coordination and cooperation in handling cyber threats. Next, it has to provide public policy to be used as a tool to investigate cyber crime activities. The last one is to provide references, recommendations and operational abilities to identify and detect cyber threats.

The second role is carried by the state and territory governments. Basically, it has the same responsibilities as federal government. The difference is that the state and territory government are focused more on the members of its own territorial area. In most jurisdictions, cyber security for individual and corporation is the domain of police department in that particular territory. The police department is focused more on the identification, investigation and prosecution of cyber crime offender. The bigger responsibility for the state and territory government, is actually to educate people, especially young adults and children, about cyber threats and how to handle it. One of the real examples regarding the implementation of cyber security in South Australia is presented by Brenton et.el [31].

The third role is carried by the ISP due to their role in providing internet services for every traffic and transaction whether it is legal or illegal. ISP has the responsibility to provide a secure line of communication for its users. One of the real actions that ISP community has conducted in cyber security is denying websites with inappropriate contents such as child abuse. They also volunteer in identifying malicious software that affected users computer, informing, and giving help and recommendations for repair. A few numbers of ISP also offer anti virus and cyber security software to its customers when they are doing online activities.

The last role is carried by the owner and administrator of ICT systems, both individual and corporate. This group has an important role due to their ability to implement cyber security system in their own facilities. If each and every one of them had implemented a strong cyber security system, malicious software would not be easily spread across systems.

C. Indonesia

In Indonesia, Kementrian Komunikasi dan Informatika (Kemkominfo) [32] is responsible to conduct communication and information technology affairs to help president of the Republic of Indonesia [33]. Related to ICT, Kemkominfo is also responsible in managing informatics applications (under the supervision of Directorate General of Informatics Applications) and post devices and informatics (under the supervision of Directorate General of Resources and the Postal and Informatics). Generally, both of them are responsible for formulating and implementing policy and providing technical guidance related to their field.

In a Directorate General of Informatics Applications, there is a specific department that is responsible for information security, named Directorate of Information Security. They are responsible for formulating and implementing policy related to management, technology, evaluation and emergency response, investigation and prosecution with information security culture [34]. For handling evaluation and emergency response, related to information security, a special team, named Government-Computer Security Incident Response Team (Gov-CSIRT) was also formed [35]. Another similar team which is responsible for more general users named Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center (id-sirti/cc) was under the supervision of Directorate General of Post and Informatics Operations [36]. Aside from the government sector, an information security community, named Indonesian Computer Emergency Response Team (ID-CERT) [37], also contracted an emergency response team. This is an independent and a community based technical coordination team.

Indonesia also has a special agency which is responsible in securing national classified information, named Lembaga Sandi Negara (Lemsaneg) [38]. This agency carries out their duties by coordinating with other government institution such as Indonesian National Police, Indonesia National Army, Ministry of Foreign Affairs, Ministry of Internal Affairs, and Ministry of Defense. In law enforcement and handling cybercrime, Indonesian National Police have a special unit who is responsible for handling special crime, including cyber crime.

III. Discussion

Generally, cyber security related tasks can be divided into four main categories. The first is formulating policies, rules and laws, what is allowed or forbidden should be defined clearly. This is what the ITU Draft [19] as legal, technical and procedural measures. The next task is education upon users, so they can interact with ICT without breaking the rules. Afterwards, users should be supervised to make sure that they comply with the rules. As a result, those who violate the law must be penalized.

From the policies of the three nations, a different scheme of delegating responsibilities among cyber related agencies were previously shown. Either from government vs. non-government perspective or federal vs. States government. Malaysia and Indonesia have a similar scheme of delegating cyber security related responsibility. Both of them apply vertical scheme of delegating responsibilities. Then, agencies or institutions who are responsible for a certain task will commit the task from the central to the local government. On the other hand, Australia divides the cyber security related tasks horizontally, between federal government and states government. The Federal Government is responsible for making rules, law and policies regarding

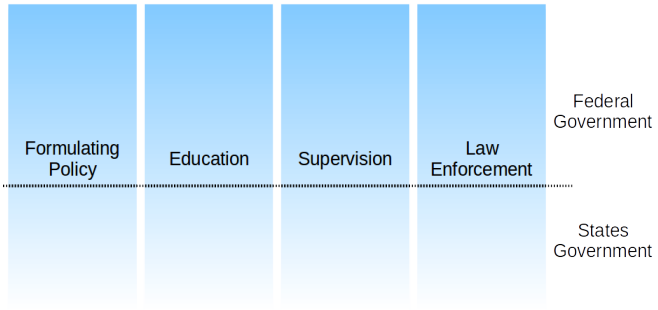

Fig. 1: Horizontal scheme of delegating cyber security related tasks

cyber security in all states. Whereas The State Government is responsible for implementing and enforcing those rules, law and policies as shown in Fig. 1.

Specifically in Indonesia, though a vertical scheme of delegating cyber security related tasks is used, some agencies involved with the similar tasks are responsible to a different director. This happens to CERT teams which were responsible to different Directorate General. The fact that each team is not directly responsible to one authority [39] could potentially cause overlapping authority between them. Therefore, a notion to establish National Cyber Agency [40] needs to be considered. National Cyber Agency, if applied, should be a single authority agency in cyber security in Indonesia. If not so, we hypothetically think that teams, organizations and institutions, who have similar interests in cyber security should be considered as a community. In the future, we will dig deeper about the strategy to empower community as a media to build a comprehensive and reliable cyber security in Indonesia, a concept known as "gotong royong" or mutual cooperation. This concept suits well as Indonesian culture is very diverse. Hopefully, this approach would be beneficial because actually the governance of cyber security already involves private sector, such as ISP and society, although they have different roles and responsibilities. Nonetheless, improvements on institutional arrangement still need to be done by Indonesian government.

References

[1] A. A. Syuhada and W. Gambett, "Online marketplace for indonesian micro small and medium enterprises based on social media," *Procedia Technology*, vol. 11, no. 0, pp. 446 – 454, 2013, 4th International Conference on Electrical Engineering and Informatics, {ICEEI} 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S221201731300368X

[2] Y. Perbawaningsih, "Plus minus of ict usage in higher education students," *Procedia - Social and Behavioral Sciences*, vol. 103, no. 0, pp. 717 – 724, 2013, 13th International Educational Technology Conference. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1877042813038378

[3] O. Yusuf, "Pengguna internet indonesia nomor enam dunia," http://tekno.kompas.com/read/2014/11/24/07430087/pengguna.internet.indonesia.nomor.enam.dunia, Nov. 2014.

[4] A. Suryadhi, "Indonesia jadi korban serangan cyber regin," http://inet.detik.com/read/2014/11/27/144319/2761037/323/indonesia-jadi-korban-serangan-cyber-regin, Nov. 2014.

[5] M. Lagazio, N. Sherif, and M. Cushman, "A multi-level approach to understanding the impact of cyber crime on the financial sector," *Computers & Security*, vol. 45, no. 0, pp. 58 – 74, 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S016740481400087X

[6] "Cybersecurity malaysia first half 2014 review report," http://www.cybersecurity.my/data/content_files/44/1309.pdf, 2014, accessed: 2015-09-13.

[7] N. H. A. Rahman and K.-K. R. Choo, "A survey of information security incident handling in the cloud," *Computers & Security*, vol. 49, no. 0, pp. 45 – 69, 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404814001680

[8] "Cyber-attacks on south korean nuclear power operator continue," http://www.theguardian.com/world/2014/dec/28/cyber-attacks-south-korean-nuclear-power-operator, Dec. 2014.

[9] A. K. Sood and R. J. Enbody, "Crimeware-as-a-service—a survey of commoditized crimeware in the underground market," *International Journal of Critical Infrastructure Protection*, vol. 6, no. 1, pp. 28 – 38, 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1874548213000036

[10] E. Hilbert, "Living with cybercrime," *Network Security*, vol. 2013, no. 11, pp. 15 – 17, 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1353485813701260

[11] N. Martin and J. Rice, "Cybercrime: Understanding and addressing the concerns of stakeholders," *Computers & Security*, vol. 30, no. 8, pp. 803 – 814, 2011. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S016740481100085X

[12] W. Kim, O.-R. Jeong, C. Kim, and J. So, "The dark side of the internet: Attacks, costs and responses," *Inf. Syst.*, vol. 36, no. 3, pp. 675–705, May 2011. [Online]. Available: http://dx.doi.org/10.1016/j.is.2010.11.003

[13] B. von Solms, "Information security — a multidimensional discipline," *Computers & Security*, vol. 20, no. 6, pp. 504 – 508, 2001. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404801006083

[14] J. Shropshire, M. Warkentin, and S. Sharma, "Personality, attitudes, and intentions: Predicting initial adoption of information security behavior," *Computers & Security*, no. 0, pp. –, 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404815000036

[15] S. L. Pfleeger and D. D. Caputo, "Leveraging behavioral science to mitigate cyber security risk," *Computers & Security*, vol. 31, no. 4, pp. 597 – 611, 2012. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404811001659

[16] D. Miyamoto and T. Takahashi, "Toward automated reduction of human errors based on cognitive analysis," in *Proceedings of the 2013 Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, ser. IMIS '13. Washington, DC, USA: IEEE Computer Society, 2013, pp. 820–825. [Online]. Available: http://dx.doi.org/10.1109/IMIS.2013.147

[17] W. R. Flores, E. Antonsen, and M. Ekstedt, "Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture," *Computers & Security*, vol. 43, no. 0, pp. 90 – 110, 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404814000339

[18] R. von Solms and J. van Niekerk, "From information security to cyber security," *Computers & Security*, vol. 38, pp. 97 – 102, 2013, cybercrime in the Digital Economy. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404813000801

[19] M. Gercke, "Understanding cybercrime. a guide for developing countries," *International Telecommunication Union (Draft)*, vol. 89, p. 93, 2011.

[20] A. K. Othman, M. I. Hamzah, and N. Hashim, "Conceptualizing the islamic personality model," *Procedia - Social and Behavioral Sciences*, vol. 130, no. 0, pp. 114 – 119, 2014, 4th International Conference on Marketing and Retailing

2013, {INCOMaR} 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1877042814029243
[21] F. K. Kalidjernih, "Healing the wound: some cross-cultural challenges to australia–indonesia relations," *Culture Mandala: The Bulletin of the Centre for East-West Cultural and Economic Studies*, vol. 4, no. 2, p. 5, 2001.
[22] R. Hardjono, "Australia and indonesia: So different yet so close," http://www.thejakartapost.com/news/2013/12/02/australia-and-indonesia-so-different-yet-so-close.html, Dec. 2013.
[23] D. binti Mohamed, "Combating the threats of cybercrimes in malaysia: The efforts, the cyberlaws and the traditional laws," *Computer Law & Security Review*, vol. 29, no. 1, pp. 66 – 76, 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0267364912002014
[24] "Mengenai mosti," http://www.mosti.gov.my/profil/about-mosti/, accessed: 2015-09-13.
[25] M. Shamir b.Hashim, "Malaysia's national cyber security policy: The country's cyber defence initiatives," in *Cybersecurity Summit (WCS), 2011 Second Worldwide*, June 2011, pp. 1–7.
[26] "National cyber-security policy (ncsp)," http://nitc.kkmm.gov.my/index.php/national-ict-policies/national-cyber-security-policy-ncsp, accessed: 2015-09-13.
[27] "Corporate overview," http://www.cybersecurity.my/en/about_us/corporate_overview/main/detail/2065/index.html, accessed: 2015-09-13.
[28] Z. Yunos, S. Hafidz Suid, R. Ahmad, and Z. Ismail, "Safeguarding malaysia's critical national information infrastructure (cnii) against cyber terrorism: Towards development of a policy framework," in *Information Assurance and Security (IAS), 2010 Sixth International Conference on*, Aug 2010, pp. 21–27.
[29] C. Brookes, "Cyber security: Time for an integrated whole-of-nation approach in australia," 2015.
[30] "Cybersecurity is the 'ultimate team sport'," http://www.federaltimes.com/article/20140708/CYBER/307080015/Rogers-Cybersecurity-ultimate-team-sport-, accessed: 2015-09-13.
[31] B. Borgman, S. Mubarak, and K.-K. R. Choo, "Cyber security readiness in the south australian government," *Computer Standards & Interfaces*, vol. 37, pp. 1 – 8, 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0920548914000750
[32] "Tugas dan fungsi," http://kominfo.go.id/index.php/node/711/Tugas+dan+Fungsi, accessed: 2015-09-13.
[33] "Peraturan menteri komunikasi dan informatika nomor 17/per/m.kominfo/10/2010 tanggal 28 oktober 2010," https://jdih.kominfo.go.id/produk_hukum/unduh/id/203/t/peraturan+menteri+komunikasi+dan+informatika+nomor+17permkominfo102010+tanggal+28+oktober+2010, 2010, accessed: 2015-09-13.
[34] "Direktorat keamanan informasi," http://aptika.kominfo.go.id/index.php/profile/direktorat-keamanan-informasi, accessed: 2015-09-13.
[35] "Profil," http://govcsirt.kominfo.go.id/tentang-idgovcert/profil/, accessed: 2015-09-13.
[36] "Struktur organisasi," http://www.idsirtii.or.id/halaman/tentang/struktur-organisasi.html, accessed: 2015-09-13.
[37] "Tentang kami," http://www.cert.or.id/tentang-kami/en/, accessed: 2015-09-13.
[38] "Tugas dan fungsi," http://www.lemsaneg.go.id/?page_id=16, accessed: 2015-09-13.
[39] G. White and N. Granado, "Developing a community cyber security incident response capability," in *System Sciences, 2009. HICSS '09. 42nd Hawaii International Conference on*, Jan 2009, pp. 1–9.
[40] A. Suryadhi, "Badan cyber nasional akan dibentuk berdasarkan keppres," http://www.republika.co.id/berita/nasional/umum/15/09/02/nu21qg284-badan-cyber-nasional-akan-dibentuk-berdasarkan-keppres, Sept. 2015.