Machfud Sidik
Sekolah Tinggi Perpajakan Indonesia
Email: machfud@stpi-pajak.ac.id

Abstrak

Makalah ini membahas masalah pengawasan yang mendasari potensi perkembangan dan risiko dalam keamanan Cyber yang diterapkan untuk industri keuangan. Serangan dunia maya pada lembaga keuangan dan infrastruktur pasar keuangan makin meluas dan lebih canggih. Cybercrime adalah ancaman yang berkembang di dunia virtual karena individu dan organisasi sektor keuangan lebih mengandalkan internet dengan kecepatan yang semakin meningkat. Kesadaran akan risiko cybercrime telah meningkat, perusahaan secara aktif mengelola risiko dunia maya dan berinvestasi dalam keamanan dunia maya, dan sampai batas tertentu mentransfer dan menyatukan risiko mereka melalui kebijakan asuransi tanggung jawab dunia maya. Pengalaman internasional menunjukkan bahwa sektor keuangan dapat mengembangkan kerangka kerja keamanan transaksi elektronik yang efektif melalui metode terbaru untuk menjaga kepercayaan publik dan stabilitas keuangan dengan menerapkan kebijakan: (i) rezim hukum yang jelas; (ii) tindakan proporsional untuk mencegah risiko integritas keuangan; (iii) rencana darurat untuk gangguan operasional; (iv) kontrol risiko dan kriteria akses dalam sistem cyber; dan (v) penelitian cybersecurity lintas-disiplin dan holistik diperlukan untuk menyelesaikan tantangan-tantangan baru yang tak terduga. Langkah-langkah seperti itu sangat penting bagi lembaga keuangan di mana difusi dan kolaborasi dengan tetap menjaga konfidensial data yang dimiliki masing-masing organisasi menjadi tuntutan yang lebih luas.

Kata kunci: Cybersecurity, Cybercrime, risiko Cyber, manajemen risiko, sektor keuangan, regulasi cyber,

I. INTRODUCTION

Technological development has improved daily life in areas such as online banking and shopping. The digital domain has become an important factor in the world and information and communication technology has proved to be a very vital factor in productivity, growth, and innovation (Rosewarne, 2014). In recent years, the world has greatly developed technologically and the development has also affected financial practices.

In early 2015, the US Director of National Intelligence, James R Clapper, ranked cybercrime above terrorism and espionage as the greatest threat to national security. GCHQ has also categorised the issue as a Tier 1 threat, indicating that cybercrime is now a high priority on the agenda of governments worldwide (Sofia de Oliveira, 2016).

Authentication, authorization, and non-repudiation are tools that system designers can use to maintain system security with respect to confidentiality, integrity, and availability. Understanding each of these six concepts and how they relate to one another helps security professionals design and implement secure systems. Each component is critical to overall security, with the failure of any one component resulting in potential system compromise.

There are three key concepts, known as the Central Intelligence Agency (CIA) triad, which anyone who protects an information system must understand: confidentiality, integrity, and availability. Information security professionals are dedicated to ensuring the protection of these principals for each system they protect. Additionally, there are three key concepts that security professionals must understand to enforce the CIA principles properly: authentication, authorization, and non-repudiation. Global cyberspace is made of complex,
multi-layered information networks which encompass the communication networks of the public sector, the business community, security authorities and control and monitoring systems used by industry and critical infrastructure which, by means of the Internet, create a worldwide network.

Society is gradually becoming an information-based service culture providing, to an ever greater extent, both public and commercial digital services to citizens. Electronic ICT networks and digital services are vital to the functioning of society. Along with the general trends of change, the advancements in technology and the utilization of the Internet, the operating environment is heavily influenced by the global nature of this increasingly expanding sector and the changing habits among users as well as the challenges associated with reliability and security. Cybersecurity risks have become more and more commonplace. Risks which were once considered improbable are now appearing all the more regularly. This trend epitomizes the new forms of instruments and methods being used in attacks, as well as ever-increasing vulnerabilities and the higher motivation of the attackers. The growing impact of cyber-attacks calls for new, creative and innovative solutions so as to mitigate the risks.

Cyber-attacks on financial institutions and financial market infrastructures are becoming more common and more sophisticated. Risk awareness has been increasing, firms actively manage cyber risk and invest in cybersecurity, and to some extent transfer and pool their risks through cyber liability insurance policies. That is Cyber-attacks are growing rapidly and pose a substantial risk to the stability of the overall financial sector. Attacks are increasing in number, scope, and sophistication, making it difficult to predict the total impact.

Cybersecurity Ventures, in a report sponsored by Herjavec Group, has predicted that the global annual cost of cybercrime is estimated to increase to around USD 6 trillion by 2021, from USD 400 billion in early 2015. Other estimates can be found by organizations such as Juniper Research and the World Economic Forum, and in a July 2017 report, Lloyd’s of London estimates that a single global cyber-attack could result in damages of as much as USD 121 billion.2 Beyond financial loss, cyber-attacks can disrupt business, financial markets and contribute to a broader loss of confidence.

Cybercrime is a growing threat in the virtual world because individuals and organizations are relying more on the internet at an increasing rate. The use of the internet and other technologies have enhanced the risk of attack from cybercriminals across the globe. With the number of incidents of theft, phishing, computer viruses, hacking, on the rise, there is a need to explore the cybercrime scenario.

The modern world is rapidly becoming more digitalized, reliant on data and increasingly interconnected. Cyber-attacks can impact all segments of life, as evidenced during the global WannaCrypt ransomware attacks in May 2017 that affected more than 200,000 computers in at least 150 countries, including those found within hospitals, utilities, railways, telecommunications and automobile companies; as well as the more recent June 2017 Petya ransomware that impacted computers within 64 countries. While the impact of the recent ransomware attacks on financial institutions was limited, the financial services sector has traditionally been the largest target due to both the attractiveness of financial gain and access to confidential financial data. According to IBM, the financial sector in 2016 was attacked 65% more often than any other sector, resulting in more than 200 million records being breached, a 937% increase over 2015 when just under 20 million were breached. Banks and other financial institutions are increasingly concerned about the sharp increase in cyber-attacks and their consequences. In an IIF survey of global banks, conducted in partnership with EY, both the Boards of Directors and Chief Risk Officers (CRO) deemed “Cybersecurity” to be a top strategic priority, second only to addressing new regulatory rules and supervisory expectations. (Institute of International Finance and EY, 2017).
It is an essential factor for CEO to ensure that management is held accountable to shareholders. It enhances the effectiveness of monitoring functions. It is posited that the more professional the CEO, the higher the degree of oversight and the more likely that members act objectively in evaluating the propensity of the company internal control and reporting practices. This indicates that a more professional the management is able to help companies sustain the continuity of business although when they are faced with financial difficulties, they are expected to propose certain action plans to mitigate the problem. An independent audit committee is highly useful to both the company and its shareholders. This independence will cause the board to work effectively on their respective duties.

Individual financial institutions have been investing heavily in control functions to counter these threats, increasing risk awareness and safeguarding critical assets and data. Authorities, in turn, have developed strategic initiatives, guidance papers and regulatory approaches to combat cybercrime and to strengthen the resilience of the wider financial system. There are also various initiatives being developed around the world that promote intelligence gathering and information sharing between public and private sector stakeholders (which, together with data, are pre-requisites for cyber-insurability). But due to the global nature, importance and interconnectedness of the financial system, and the sharp rise in cyber-attacks, there has been an increasing focus on what impact such attacks could have not only on individual institutions but also the stability of the overall financial sector. Over recent years, the types of perpetrators of cyber-attacks have expanded and their skills and sophistication have significantly increased.

These perpetrators can belong to hacking groups or to criminal gangs but they may also be state-sponsored as part of a broader and more powerful attempt to destabilize other jurisdictions by, for example, disrupting their networks (i.e. electricity) or infiltrating their systems (i.e. communications system, financial system, etc.)

One such example is North Korea, which is alleged to have sponsored several attacks, including both the already mentioned Wanna Crypt ransomware and the attempted heist of USD 1 billion from the Bangladesh Central Bank in February 2016. According to TIME, North Korea employs an army of 6,800 state hackers that generate an annual revenue of USD 860 million. Their mission is both to cause physical or economic damage to their targets, and to obtain revenues to help finance their nuclear program.

The motives of perpetrators vary widely but could be organized into four broad categories:

a. Cyber-crime: the motivation is a financial gain (e.g. attacks that seek to steal money);
b. Cyber-espionage: gain information on another organization in pursuit of leverage (e.g. political, financial, capitalistic, market share, etc.);
c. Cyber-hacktivist: involves stealing information to serve a political agenda; and,
d. Cyber-war: the notion of a nation-state’s effort or transnational threat to compromise/coerce an adversary via a cyber-attack.

Regardless of the actor, the tools used or the motives they might have, any attack on critical components or services of the financial system, could have either direct or indirect impacts that could threaten the stability of the system, or of its respective participants. For this reason, the threat of cyber-attacks is no longer an IT or operational risk within financial institutions, and has expanded into broader more holistic categories, such as "enterprise risk" and "system-wide risk." But unlike financial risks, such as credit or market risk, and given the novelty and constantly evolving nature of cyber-attacks and the lack of empirical data, cyber-risk cannot easily be modeled, measured, or hedged based on past performance, as can be done with credit risk, for example. Financial institutions are already employing
many measures to reduce the impact of cyber-attacks, including having a good understanding of cyber-resilience, adopting a comprehensive and forward-looking approach to manage cyber-risk, implementing the right controls and responsive actions available for mitigating a security failure and engaging in swift cyber-threat information sharing. The transformation process that financial institutions, financial markets, and financial infrastructures are undertaking to adapt to the new "digital future" will exacerbate cyber-risks.

II. RISKS AND OVERSIGHT ISSUES

The threat and impact of cyber-attacks on the financial sector are increasing, and financial sector authorities are increasingly looking to address cyber risk and cybersecurity. Improving coordination between financial sector authorities and other agencies dealing with cyber risk and cybersecurity is essential. Establishing coordination protocols between financial sector authorities and other agencies involved in regulating and supervising cyber-risk, akin to those in place for financial stability. Some jurisdictions ask financial institutions to develop an ICT strategy and risk management framework, including incident response plans with a clear chain of command to take the necessary business decisions. Some countries also require the appointment of an information security officer.

The mandatory or suggested practices identified in this paper are those of primary interest for the financial sector authorities in charge of regulating and/or supervising licensed banking and nonbanking institutions. As more dimensions of the provision of financial services migrate to the space of interconnected computers (or “cyberspace”), other state and regional agencies — such as European Union Agency for Network and Information Security (ENISA), and national security agencies in some jurisdictions — will be regulating how operations are to be conducted in their respective domains. This implies that financial institutions in some jurisdictions will have to abide by a growing number of regulations pertaining to technical ICT matters beyond the regulatory perimeter of the financial sector authorities, such as encryption protocols, application programming interfaces (APIs), or authentication mechanisms.

Many countries have already published national cybersecurity strategies, frequently identifying the state agencies in charge of setting minimum standards and responding to a cyber-incident. References to bank security can already be found in several country strategies. National cybersecurity strategies and legal frameworks should clearly specify the respective responsibilities of the financial sector and other authorities, such as national security agencies. Without such clarity, jurisdictional conflicts are bound to arise when issuing new cybersecurity regulations or, even worse, when handling cyber incidents in the financial sector. A new reference guide is being developed by a host of organizations to serve as a single source to guide countries in developing their own national cybersecurity strategies. This guide should also help financial sector authorities better understand the nature of the institutional structure required to deal with cybersecurity. It is currently being prepared by the International Telecommunication Union (ITU), a United Nations agency, in partnership with several cybersecurity organizations in the world.

Taxonomies are languages or conventions for information sharing, and there are many of them. For instance, ICT specialists frequently work with MITRE Corporation’s “Common Attack Pattern Enumeration and Classification” (CAPEC), a “comprehensive dictionary and classification taxonomy of known attacks that can be used by analysts, developers, testers, and educators to advance community understanding and enhance defenses”. Regarding mechanisms of attack, CAPEC identifies 118 different mechanisms to collect and analyze information; 152 to inject unexpected items; 156 to engage in deceptive interactions; 172 to manipulate timing and state; 210 to abuse existing functionality; 223 that employ probabilistic techniques; 225 that subvert access control; 255 that manipulate data.
structures; and 262 that manipulate system resources. Regarding domains of attack, CAPEC identifies 403 different types of social engineering; 437 on the supply chain; 512 on communications; 513 on software; 514 on physical security; and 515 on hardware (The World Bank Group on Financial Sector’s Cybersecurity: Regulations and Supervision, 2018).

The Indonesian government should develop the national cyber strategy to protect national assets and cyberspace environment. The strategy is created to ensure an alignment process within government agencies. The strategy must have principles. (i). Leadership: Complexities and challenges of cybersecurity in Indonesia need powerful leadership. The Leaders must recognize and respond with the importance of cybersecurity in their agencies. (ii). Shared responsibilities: Cybersecurity requires a shared responsibility because the use of ICT is related to each other. Each agency must maintain their sensitive ICT resources. (iii). Partnership: To create a cybersecurity, it is required the cooperation and partnership from the various parties. (iv). National Values Impact and Risk Management: Applying a business impact analysis approach for national asset and risk management. This approach aims to prioritizes the protection of the national assets and critical ICT resources.

According to above principles, below are the strategies that should be considered by the Indonesian government to improve national cybersecurity i.e. Create and alignment cybersecurity regulations. (v) A Regulation is a basic foundation to protect the cyber environment. A regulation also must be aligned with other laws. It must be developed and revised regularly to anticipate rapid technology development. Further is the commitment of all parties for law enforcement. Strengthen the roles, responsibilities, and authorities of cybersecurity government organizations: To solve the problems of cybersecurity in the national level, it is needed cooperation and collaboration with academics, governments, business organizations, and communities. Therefore, at the strategic level, there must be an organization that responds to supervise and coordinate cybersecurity organization. This organization must be supported by the highest authorities at the national level, politically and technically. At the operational level, the country also needs technical agencies to handle incident management in each sector. (vi). All of the cybersecurity organizations must have clear roles, responsibilities, and authorities. It is a very important part because all of the complex problems of cybersecurity can be solved only by the powerful organization and mutual cooperation. The cybersecurity organization also needs the human resources who have integrity and ability in cybersecurity. (vii). improve cybersecurity human resources: Training and skill development is needed to improve quality and to increase quantity. Government agencies can develop their human resources by doing cooperation with universities and training institutions. (viii). Development application, systems, and technologies security standard.: The autonomy on developing application, system, and technology are needed to protect the country from internal and external cyber threats. But, it must be standardized and evaluate regularly. (ix). Improve security awareness and governance: Introducing risks that exist in cyberspace will raise the awareness about the importance of cybersecurity. The efforts to develop awareness can be done through campaign, dissemination and publication program. Implementation of security governance is also the important part. It can be adopted from national standard or international best practices of security governance standard.

Apart from these formal constructs, banks also need to be practical. Adopting procedures to deal with suspicious employees, taking actions to address a lack of internal forensic computer expertise, purchasing sufficient liability insurance coverage for adverse electronic events, and implementing crisis teams are all basic issues that banks need to consider in addressing any comprehensive security system. Technical consultants can help provide any bank with a complete blueprint for action on this front. However, the banking industry can use some basic protection methods and specific defensive tools to minimize their risks from cyber-crimes. In general, a bank needs to use some sound logic and not to overreact or panic in developing protection mechanisms. Three good places to start are an...
effective risk assessment and a review of the policies and procedures related to security. The risk assessment, if done appropriately, will direct the rest of your actions and lead to effectiveness. First, get some professional assistance, if necessary, but make sure your bank has analyzed all possible threats and risks associated with cyber-crimes and similar malicious activities. Even when your resources are limited, identifying all the risks is inherently valuable. That allows management to ‘prioritize’ the risks with high probability and high impact or costs (if a crime occurs). This prioritized list then provides a cost-effective means of mitigating the risks. Second, the bank can implement prevention techniques, tools, and policies. The tools would include technologies to protect the bank’s system and network from malicious objects and attacks, such as firewalls, intrusion detection system, anti-virus software, and antispyware procedures. It also would include a strong public education campaign to minimize the risk of phishing and ID theft. Third, a bank should ensure it has a sound business recovery plan in its policies and procedures in case an attack occurs and succeeds. Several things can cause a bank to lose its computers and information systems, including system failures, disaster (man-made or natural), hackers/crackers and other cybercriminals. An effective business recovery plan will allow a business to recover from any of these unfortunate events. It is essential that the recovery system, especially data recovery, be tested before relying upon it. Fourth, develop an incident response plan as part of the policies and procedures, if applicable. An incident response plan should be developed for any risk that exceeds ‘minimum’ risk. What if some cracker or cybercriminal attacked your bank successfully and did the one thing that has the highest public risk for the bank (for example, stole thousands of credit card numbers and PINs, wiped out your hard drives, stole the corporate identity, etc.)? How would your bank respond to that attack and the resulting bad publicity? There is no substitute for the preparation and planning for such an event, and an appropriate incident response plan does just that. Fifth, education (viz., training, seminars, etc.) is critical to developing an effective level of awareness regarding the types of risks, knowledge of the “red flags” for which to watch, and a vigilant defense necessary for at-risk businesses, such as banks. Education includes both consumers and employees, and their ability to recognize the types of cybercrimes and respond appropriately to each. A key control point in detecting and preventing cybercriminal tactics (for example, phishing, ID theft) is the bank’s own employees, especially frontline staff (for example, the information systems help desk). Last but not least, banks can use some specific information technology (IT) or information systems (IS) countermeasures to mitigate the risk of cyber-crime. For example, a U.S. banker recommends “fraud detection software, voice print recognition, and smart chips to replace magnetic stripes on cards.” Similarly, the FDIC recommends “scanning tools, e-mail authentication (an example would be digital signatures) and user authentication (an example would be voice print).” The FDIC report “Putting an End to Account-Hijacking Theft” provides extensive details on these suggested IT defenses.

A bank, therefore, needs a broad strategy of prevention. "No one method can protect a bank against all types of cyber-crimes and cyber-enabled perpetrators." Because of the high level of risk in banking related to cyber-criminal activities, banks must maintain constant vigilance and diligence to be aware of the risks, assess and prioritize the risks, and take appropriate actions to mitigate the risks. One of the general issues in the development of cyber-laws is the nature of cyberspace itself, which is new and young. Traditional laws, thus, will not be effective in tackling the various types of activities conducted on the cyber-space. For example, deception of the computer, or theft of electronic data cannot be dealt with under the traditional penal laws in many countries. That is why certain countries like India, Malaysia, and others began to enact the new "Information Technology Act" and "Digital Signatures Act," respectively. The other issue is the jurisdiction of the courts and applications of the laws due to the nature of the cyber-space beyond national jurisdiction. In order to survive and grow in a global competitive scenario, the time has already come when the security aspects of the banks must be dealt with on a priority basis. Timely and adequate execution of the cyber resilience strategy is critical for many countries financial stability.
Cybersecurity continues to be an issue of intense interest governments and our customers; and with the passage of time, it has only become more so. The imperative that many financial institutions emphasized in developing cybersecurity in last decade remains important, but insufficiently realized across the whole of industry; it is only by working together internationally, as vendors, customers, and policy and lawmakers, will we make a substantial difference in addressing the global cybersecurity challenge. While there is still no simple answer or solution to the cyber security challenge, it is increasingly apparent that there are steps the global community can take – as well as individual organizations – to drive demonstrable progress in reducing cyber security risk, including that of collaborating so as to reach an agreement on principles, laws, standards, best practices, norms of conduct, and protocols – with recognition that trust has to be earned and continuously validated. There are a number of steps that financial institutions can take to improve the robustness of their defences to cybercrime: better understanding of the problem through partnerships; investing in technology such as analytics platforms; and sharing information that may be relevant to others.

First, there is growing agreement among financial institutions that cooperation should be encouraged between the public and private sectors, and many such initiatives have already been put in place. The establishment of initiatives, such as the Cyber-security Information Sharing Partnership (CISP), demonstrates an increased realization that cybersecurity threats cannot be addressed in isolation and that co-operation between stakeholders is key.

Second, supporting investment in technological advances is also crucial for improving the robustness of defenses to cybercrime. Although appearing legitimate, the emails contained malware that opened remote access to bank computers and allowed criminals to infiltrate the system. In response to these kinds of risks financial institutions are beginning to recruit staff with strong security backgrounds to improve employees’ awareness of threats and reduce reliance on technology to stop breaches. The majority of efforts are being channeled into updating ICT security with innovative software and analytics as well as forensic skills and the means to trace potential attackers. However, a number of experts from the sector recently emphasized that this investment must be better guided and informed by people who understand the specific needs of each business and can therefore identify which technology is most appropriate for it. The type of technology adopted should, in addition, be capable of processing and identifying human factors and their impact on the wider system.

In the era of globalization, cyberspace has become a staple of human life, and it connects people regardless of the distance. Cyberspace is a new world brought forward by the internet. Paul Wagner (2010) argues that cyberspace is beyond every computer system that’s connected by wire. Cyberspace also includes: (i) isolated networks (private, corporate military); (ii) laptops and other personal PCs connected some of the time (wireless, modems); (iii) industrial control machinery, including programmable logic controllers (PLCs); industrial robots (connected to PLCs or directly to computers); (iv) home control equipment (home appliances and their control units); (v) mobile devices (smartphones, PDAs); and (vi) USB and other storage devices.

With the advent of computers (and especially the Internet) businesses are subject to threats of malicious activities and cyber-crimes. Cybercriminals use computers and technology to carry out the destructive activities that have been around for decades. Whether it is insiders or unknown intruders involved in hacking (i.e., the unauthorized use or attempt to circumvent the security mechanisms of an information system or network), cracking (i.e., breaking into a computer system), phishing (i.e., attempting to acquire identifiers and passwords), or phreaking (i.e., cracking a phone or communication network), as long as people are the weakest link, there really is no safe harbor from cybercrime.
Cyberspace displays reality, albeit not a tangible one. It is a virtual world, virtual reality, and a world without borders. This is what is meant by the borderless world in a way that cyberspace does not recognize state borders, and it eliminates the dimension of space, time and place (Purbo, 2000, p. 50). It enables its citizens to connect with anyone anywhere as Bruce Sterling (1992) argues: Although it is not exactly "real," "cyberspace" is a genuine place. Things happen there that have very genuine consequences. This "place" is not "real," but it is serious, it is earnest. Tens of thousands of people have dedicated their lives to it, to the public service of public communication by wire and electronics. The concept of cybernation sparks the hope of bringing convenience, happiness, and endless opportunities for people. However, it comes with a price. Cybersecurity is a real and urgent necessity since its effects could potentially damage or disrupt people's lives, states, and even the whole world depends on how well-developed a state law is and how much it is concerned with the advancement of technology. This was revealed at the UN Congress in Vienna: Reasons for the lack of attention to cybercrimes may include relatively low levels of participation in international electronic communication, low levels of law-enforcement experience and low estimations of the damage to society expected to occur from electronic crimes.

Although with the advent of technologies, the banking sector has been able to reach more customers, however, it has also enhanced the risk for customers who often feel reluctant and insecure in opting for such services. There is a need for the banks to evaluate their current operating practices. In this paper, the researcher makes an attempt to study the cybercrime scenario and its impact on the banking sector.

Cybercrime according to Douglas and Loader (2000) can be defined computer-mediated activities conducted through global electronic networks which are either illegal or considered illicit by certain parties. In the banking sector, the cybercrimes which are committed using online technologies to illegally remove or transfer money to different account are tagged as banking frauds (Wall, 2001). The cybercrimes according to Wall (2001) can be categorized into four major categories i.e. cyber-deceptions, cyber-pornography, cyber-violence, and cyber-trespass. The banking frauds are sub-categorized in cyber-deception which can be defined as an immoral activity including stealing, credit card fraud, and intellectual property violations (T., Brian Yeh Legislative Attorney May 27, 2016).

There is a number of frauds or cybercrimes witnessed in the banking sector, like ATM frauds, Cyber Money Laundering, and Credit Card Frauds. However, in general, all the frauds are executed with the ultimate goal of gaining access to a user's bank account, steal funds and transfer it to some other bank account. In some cases, the cybercriminals use the banking credentials like the PIN, password, certificates, etc. to access accounts and steal a meager amount of money; whereas in other cases they may want to steal all the money and transfer the funds into mule accounts. Sometimes, the intention of cybercriminals is to just harm the image of the bank and therefore, they block the bank servers so that the clients are unable to access their accounts (Claessens et al., 2002).

As a lot of vulnerabilities exist in the defense system of the banking sector, thus there is a need to investigate the ways to increase awareness about the measures that can be undertaken to combat cybercrimes in the banking sector. However, not many studies in the past have been conducted in this area which would suggest ways to mitigate the risks and combat such crimes. Hence, some types of businesses, no doubt, are more susceptible to cyber-crimes. Vulnerable businesses include insurance, communications/ media, defense contractors, healthcare, technology, high-profile businesses, and financial institutions. In addition, governments are vulnerable too. The risks are probably as high or higher for the banking industry as for any other.

As per the OECD report (2007), these malicious exploiters can be categorized into five subcategories. Innovators (who seek to find security holes in the system to overcome protection measures adopted by the banks). Amateur (who are beginners in this area and
their expertise is limited to computer skills, which is exploited by the cybercriminal). Insiders (who are working within the bank to leak out important information in order to take some kind of revenge). Copycats (they are interested in recreating simple tasks). Criminals (highly organized and very knowledgeable who may use all the above-mentioned stakeholders for their own profit).

As per the definition is given by OECD report (2007), money mules are individuals recruited wittingly and often unwittingly by criminals, to facilitate illegal funds transfers from bank accounts. According to the FBI (Federal Bureau of Investigation), these individuals engage in the money transfer activity in exchange for some percentage of that money. According to Florêncio and Herley (2010), their role is to convert reversible traceable transactions into irreversible untraceable ones.

Victims, according to OECD (2007), in the banking sector can be categorized into two categories; banks and users of these banks. The users or customers can be individuals, SMEs, or large multinational organizations. The most negative externality among the legitimate actors is created by individual users and SMEs who do so by not employing risky online behavior or by not employing security measures during transactions (Asghari, 2010; Mannan & van Oorschot, 2008).

They are the most important actor of this system as they improve the existing banking system and help in removing the vulnerabilities and development of systems so that banking frauds can be mitigated. The security guardians in case of the banking sector could be the bank itself or some third party hired by the bank in order to ensure security from such threats.

The banking industry across the globe is facing a challenging situation which is thought-provoking due to the geopolitical and global macroeconomic conditions. The banking sector is forced to evaluate its current practices in order to analyze and manage their risks effectively. Technology-driven approaches have been adopted for the management of risk. Due to the growth of IT, penetration of mobile networks in everyday life, the financial services have extended to masses. Technology has made sure that banking services reach masses as it made these services affordable and accessible.

In order to fight these cybercrimes, the banking sector needs to collaborate with global authorities and watchdog organizations so that a model can be developed which can help in controlling and dealing with such threats. The main issue of concern here is that there is an absence of effective compilation service in the banking sector which can identify the trends in cyber-crime and compile a model according to it. However, in the last few months, banks all across the globe have perceived cybercrime as among their top five risks (Stafford, 2013). High profile banks in the UK like Barclays and Santander were targeted by hackers who stole personal information of nearly 2.9 million credit card customers by hacking the software maker system of these banks, which led them to incur huge losses. However, the scenario is not restricted to the UK, in the US as well such attacks have surfaced in the past years and in order to curb the effect, they launched the program Quantum Dawn 2 which test the efficacy of system installed in banks in response to cyber-attacks (Stafford, 2013).

III. CYBER SECURITIES APPLIED IN INDONESIA

Indonesia is a little left behind in keeping up with the development of information technology, as a result of an improper strategy of technology development that ignores scientific and technology research. Consequently, the technology transfers from developed industrial countries is not followed by the mastery of the technology itself that turns Indonesia into a non-technological-based country. Alternatively, puts it, "Indonesia is a new
pseudo-industrializing country. "The fact that Indonesia is still left behind in information technology raises the question of the condition of the implementation of cybersecurity policy in Indonesia.

Indonesia is in the early stages of developing a national cybersecurity strategy. The legal framework for cybersecurity in Indonesia is weak. There is no clear classified security law or policy, and security practices are spread across different legislation. There are no specific cybersecurity provisions in place. ID.SIRTII/CC, the national CERT, seems to be in the early phases of operation. ID.CERT is a non-government CERT, but has been operating for longer. There is no dedicated cybersecurity public-private partnership in Indonesia, so the CERT acts as the main liaison body for the private sector. Industry representative associations exist, but none are dedicated to cybersecurity in particular. Indonesia lacks any joint public-private sector plan to address cybersecurity. Indonesia subjects cybersecurity service providers to a range of burdensome laws and policies, including discriminatory procurement preferences, local testing requirements, and limits on data flow. Indonesia has been developing its economic capacity, among others, through investment in the ICT sector. Data from the Ministry of Finance of the Republic of Indonesia shows an increase of approximately 18.24% or equivalent to USD 219 million in the realization of Central Government ICT Expenditure in the period Fiscal Year 2009-2010. ICT growth is also felt by Indonesia people. This is shown by a high number of mobile phone users, which is about 180 million. Indonesia also includes the biggest users of social media in the worlds, Facebook user third biggest in the world and the fifth for twitter users. Statistical data showed that Indonesia runs into a rapid growth of the ICT sector. A rapid development in the ICT sector gives a positive impact on economic growth and also a big threat to cybersecurity in Indonesia. The current threat for every country is not only come from physical threat, but also from the cyber threat because the cyber threat potentially destroying the economy and destabilize the country’s security. To anticipate the threats that come from cyberspace, the government needs to develop a defense and security system and strategy.

In general, the elements that can be identified as potential sources of threats consist of internal and external sources, intelligence activities, disruption, investigation, extremist organizations, hacktivists, organized crime groups, rivalry, hostility and conflicts, as well as technology (The Ministry of Defense of the Republic of Indonesia, 2013, p. 24). Almost every country believes that science and technology are two important factors in supporting the growth and progress of a country. In the context of economic development, technology can act as an engine of economic growth. Countries that do not have and master science and technology will be left behind. Science and technology are now glorified and have become an ideology. Some people worship technology so much and treat it as if it was the only way to welfare, prosperity, and justice.

A weak cyber defense may create tensions among countries and disrupt the stability of security, create social, economic, and environmental impacts, as well as disrupt the relationship among countries (Schjolberg, Stein and Solange Ghernaouti-Hélie, 2009). Cybersecurity has two keywords: cyber and security. Talking about cyber means talking about information, connections (telecommunications, networks), gateways (computers, devices, users), rooms, or spaces, and it is about involving, using, or relating to computers,
networks, and the internet. Meanwhile, security is usually related to assets and assets protection. Security is protecting the asset, protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction, protecting information and systems from major cyber threats (Schjolberg, Stein and Solange Ghernaouti-Hélie, 2009). Computer security, cyber security, or IT security is information security applied to a computer or a network. Computer security aims to help users prevent fraud or detect any attempts of fraud in an information-based system. The information itself is non-physical. Cybersecurity is an effort to protect information from cyber-attacks. Cyber-attacks in information operation mean all deliberate actions to disrupt the confidentiality, integrity, and availability of information. This action can be in a form of physical disruption or a disruption of the logical flow of information system. A cyber-attack is an attempt to disrupt information which focuses on the logical flow of an information system. National Cyber Security is a term used for cybersecurity that is related to the assets/resources of a country. The objective of national cybersecurity is the protection, domination, and control of data and information. National cybersecurity is closely related to information operation, which involves various parties such as the military, the government, state-owned enterprises, academia, private sectors, individuals, and the international world. The continuity of information operation does not only rely on cybersecurity itself, but it also depends on physical security, which is related to all physical elements such as data center buildings, disaster recovery system, and transmission media.

In terms of cybersecurity, Indonesia already has a system and strategy of cybersecurity conducted by government agencies and also the official community. Cybersecurity policy is coordinated by the Ministry of Communication and Informatics (MCI). There are three government organizations involved in cybersecurity in Indonesia, which are Information Security Coordination Team, Directorate of Information Security, and Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII). The Information Security Coordination Team was formed in April 2010 to coordinate cybersecurity, focusing on the expertise and the practice in the field of information and technology. The Directorate of Information Security has the tasks of policy formulation and implementation, training, monitoring, evaluation and reporting in the field of information security governance. Lastly, ID-SIRTII was established by the government based on Regulation of the Minister of Communication and Informatics No. 8 of 2012 to handle security on internet infrastructure. Meanwhile, there are two community organizations involved in cybersecurity in Indonesia. Acting as a supporting institution, Indonesia Communication Emergency Response Team (ID-CERT) is an organization that works with the government in special cases to support the development of cybersecurity in Indonesia. In addition, IDCERT also functions as a supporting institution for government organizations (Setiadi, Sucahyo, & Hasibuan, 2013) such as the ID-SIRTII. Another community organization is the Indonesia Academic Computer Security Incident Response Team (ID-ACAD-CSIRT), the organization for the universities that want to focus on the development of security in Indonesia. ID-ACAD-CSIRT currently has 40 members of academic CSIRT universities. The government of Indonesia has created a policy concerning the implementation of cybersecurity in its legislation based on the Law No. 11 of 2008 on Electronic Information and Transaction (ITE). There are several other laws that are indirectly related to the policy, but related to such information, such as the Law No. 36 of 1999 on Telecommunication, and the Law No. 14 of 2008 on the Openness of Public Information.
To deal with the problem, several leading jurisdictions have issued or proposed detailed laws, regulations or guidelines dealing with cyber risk or, more generally, ICT risk. Regulations in the Financial Sector, which coincides with those of the G7’s fundamental elements. It also outlines attempts to identify the emerging consensus on practices to implement regulations, as well as on how to supervise their implementation by individual financial institutions.

Indonesian cybersecurity policy was initiated back in 2007, following the release of the Regulation of the Minister of Communication and Informatics No. 26/PER/M.Kominfo/5/2007 on the Security of the Use of Internet-protocol-based Telecommunication Network, which was later replaced by the Regulation of the Minister of Communication and Informatics No. 16/PER/M.Kominfo/10/2010. This was then updated with the Regulation of the Minister of Communication and Informatics No. 29/PER/M.Kominfo/12/2010. An important aspect in the regulation is the establishment of ID-SIRTII. The Minister of Communication and Informatics assigned the team to help control the security of Internet-protocol-based telecommunication network. ID-SIRTII's functions and tasks are to watch and to detect early and warn when any disruptions on the network occur. The team also coordinates with related parties at home and abroad when it needs to secure the network. The team also provides information when threats and disruptions come up. Finally, IDSIRTII also works on devising work plans (Article 9 of the Regulation of the Minister of Communication and Informatics No. 29/PER/M.Kominfo/12/2010). According to Hasyim Gautama, the framework of cybersecurity law in Indonesia was based on Law No. 11 of 2008 on Electronic Information and Transaction, Government Regulation No. 82 of 2012 on the Implementation of Electronic System and Transactions, as well as ministerial circulation letters and minister regulations (Ardiyanti, 2014).

Aside from the initiation of cybersecurity-related legislation, to ensure legal certainty in the development of cybersecurity, the government enacts the cybersecurity national framework. However, the legal framework for cybercrime-handling is still weak. Despite the existence of the law that forbids any forms of attacks or vitiation to the electronic system, no law that specifically regulates and contains cybercrime is available. Meanwhile, cybercrime evolves and takes place rapidly, making it hard for the law enforcers to handle it.

Cyberspace crimes or known as cybercrime include identity theft and data (information resources), piracy accounts (email, IM, social networks), the spread of malware and malicious code, fraud, industrial espionage, hostage-critical information resources and cyber warfare or war in cyberspace. Convention on Cybercrime has been split into several sections or called by the typology of cybercrime, such as 1) Offences against the confidentiality, integrity, and availability of computer data and systems 2) Computer-related offenses 3) Content-related offenses 4) Offences related to infringements of copyright and related rights 5) Ancillary liability.

The cybercrime that is attack national assets and disrupts national interest, it is called cyber terrorism, or cyber warfare. As said by Colarik cyber terrorism means premeditated, politically motivated attacks by subnational groups or clandestine agents, or individuals against information and computer systems, computer programs, and data that result in violence against non-combatant targets and definition of cyber warfare is Information
warfare is defined as a planned attack by nations or their agents against information and computer systems, computer programs, and data that result in enemy losses. Both cybercrime and cyber warfare have occurred in Indonesia, the cases of cybercrime and cyberwarfare that possibly occurred in Indonesia are Data Theft, Release of Private Data, Copyright Violation, Defacing and Patriotic Hacking. Theft of confidential and sensitive information data via portable media such as external storage, CD/DVD, the memory card is often the case in Indonesia. Theft occurs because the data is not stored with good security or the negligence of the owner. The sample for this case is the release of private video artists in 2010, which scandalize public. Piracy rates in Indonesia are still high, because of the lack of law enforcement. Indonesia became the highest state in the rate of software piracy. This is a serious issue for the government that needs to be resolved for improving the content and software industries in Indonesia. Geographically, Indonesia is very large and bordered with another country. This issue could be a potential conflict because usually disputes in cyberspace begin with the ownership claims between the two countries. Claims ownership of culture and territory and also labor issues spread to the conflict in cyberspace. Cyber conflict begins from threads in a cyber-forum that blamed each other and continued by attacking the others government websites.

The terms computer crime, high-tech crime, digital crime, e-crime, and cyber-crime can be used interchangeably with electronic crime. E-crimes are essentially crimes where the computer is used either as a tool to commit the crime, as a storage device, or as a target of the crime. As a storage device, computers can either store information that will assist in the execution of the crime or information that is illegal for the owners to possess, such as stolen intellectual property. Computers are classified as a target if the information that they contain is altered or retrieved in an unlawful way, such crimes can range from amateur hacking to terrorism.

Phishing relies on the ability of the perpetrator to fool (or con) a victim, and that usually involves ‘spoofing’. Spoofing is the imitation (or mimicking) of a legitimate Web site, e-mail or entity communication in order to trick the recipient into believing the communication or website is trustworthy. Thus, phishing involves the use of seemingly legitimate communications (that is, spoofed) to deceive bank customers into disclosing sensitive information, such as bank account information, social security numbers, credit card data, passwords or financial personal identification numbers (PIN). Most often, the purpose of phishing is to gain sufficient information to perpetrate a fraud.

According to the ITU (International Telecommunication Union) Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. From this definition, cybersecurity means a mix of components to protect the environment and assets, the components such as policy, technology, etc. ITU also categorized national cybersecurity into five dimensions. This section explains dimensions of cyber security in Indonesia based on cybersecurity agenda for development country by ITU. Dimensions were assessed from the aspects (1) Legal Measures, (2) Technical and Procedural Measures, (3) Organizational Structures, (4) Capacity Building and (5) International Cooperation.
The 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 policies and regulations. Telecommunication Act (UU Telekomunikasi No. 36/1999) and the Information and Electronic Transaction Act (UU ITE No. 11/2008) are two acts that directly related to ICT security. Those acts become the basic foundation for formulating regulations and policies related to information security. The numbers of related policies and regulation on ICT security are still very limited to protect the rapid growth of the ICT sector in Indonesia. Indonesia has only two acts that describe security in the ICT sector. Compared with another countries, Indonesia lagged behind in ICT security policy and regulation, such as Malaysia that has already had computer crime act (1997), digital signature act (1997), telemedicine act (1997), communication and multimedia act (1998), payment system act (2003), personal data act (2010), etc., even other country like Slovenia have PDP act (2004) and E-commerce & E-signature act (2004) while Estonia have Estonia-Digital Signature Act (2000) and Electronic Communication Act (2004).

Because of the limitations of the act, criminal cases related to cybercrime in Indonesia could also be punished with criminal procedural law codex (UU KUHAP), Pornography Act (UU Antipornografi No. 44/2008), Copyright Act (UU Hak Cipta No. 19/2002), and Consumer Protection Act (UU Perlindungan Konsumen No. 8/1999). Another Cyber law that is still in the formulation stage between the government and legislative is the Information Technology Crime Act (RUU Tindak Pidana TI/TIPITI) and Multimedia Convergence Act (RUU Konvergensi Multimedia). Applying the standard is an important step to protect the security of information in cyberspace. Those standards will become a reference for each sector to enhance the capabilities in the field of information security. The Indonesian government has been aware of it by adopting international standards on security management (ISO 27001). Indonesia National standards for security management called SNI ISO/IEC 27001:2009, which will be explained in the following sections together with existing government and community programs and activities.

The following is an explanation of technical and procedural measures that developed by governments and communities in Indonesia: (i). Indonesia National Standard (SNI ISO/IEC 27001:2009: Information Security Management System): Government of Indonesia in this regard the National Standardization Agency (BSN) has established an identical adoption of ISO 27001 become SNI ISO/IEC 27001. This standard covers all types of organizations such as commercial enterprises, government, and nonprofit organization. This standard specifies requirements for establishing, implementing, operating, monitoring, assessment, improving and maintenance of Information Security Management System (ISMS) is documented in the context of the overall organization's business risks. This standard specifies requirements for the application of security controls customized to the needs of each organization or the organization. ISMS is designed to ensure the selection of security controls are adequate and proportionate to protect information assets and give confidence to interested parties. (ii). Health and Safe Internet Program: To optimize information security in cyberspace, Ministry of Communication and Information Technology (MCIT) has made government program called health and safe internet program. This program contains educational and public awareness about the importance of information security. It is hoped that through this program, a community in ICT sector participates in maintaining security in cyberspace. iii.
Trust+: Trust Positive (Trust+) is negative content filtering technology based which is developed by models and the workings of this system are to perform filtering of the top level domain, URL and Content, Keyword, Expression. Implementation Trust+ is performed in MCIT, telecommunications operators and ISPs. iv. Internet devises Health & Safe for Children Indonesia (Perisai): Perisai is Open Source software designed to provide protection and education for the children of Indonesia. This software is as the result of the cooperation of MCIT, Ministry of Research and Technology, IGOS Center and PC LINUX. Perisai distributed freely and easily to use by children because of the government very aware that the protection of negative content should be done as early as possible. Nawala Project: DNS filtering protection that protects internet connection from negative content such as pornography, gambling, phishing, malware, or anything harmful. This service can be used with free of charge, just by configuring DNS address in accordance with predetermined. This Project is developed by the ICT community in Indonesia to help the government enforce the laws, values and social norms.

Currently, there are several organizations, institutions, agencies or teams involved in information security in Indonesia. Organizations established by the government or agency set up by the community. As shown in Figure 1, at the national level, MCIT has the authority in preparing the organization that handles information security sector. There are three government organizations involved in information security in Indonesia, Information Security Coordination Team, Directorate of Information Security, and Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII). ID-SIRTII is the first institution established by the government to handle security on internet infrastructure. The function of this organization is really crucial in ensuring the conducive environment on the Internet to overcome such negative impact brought by the tremendous development of Internet into communities especially that involve intellectual property right and Internet content.

Furthermore, MCIT in April 2010 formed the coordination team of information security to accommodate the importance coordinate and collaborate in the government agency. Information Security Coordination Team composed of leaders of government agencies associated with security, also experts and practitioners of information security. Still, in the same year, MCIT formed of structural organization of information security called Directorate of Information Security. Meanwhile, ID-CERT is an organization that advocates and security incident response coordination in Indonesia. ACADEMIC CSIRT (ID-ACAD-CSIRT) is an organization for the University who want to focus on the development of security in Indonesia, currently has 40 members Academic CSIRT University. ID-CERT and ID-ACAD-CSIRT even though there is no structural line with the government, those institutions continue to work with governments to support information security in Indonesia.

Capacity building capabilities contribute to creating the information security components. The capacity can be gained through human resource development, organizational development, and institutional and legal framework development. Here are the efforts made by the government to develop capacity in the information security aspects.

Politically, Indonesia has a free and active principle, it is stated in the preamble of the constitution. Indonesia has collaborated with international parties on the issue of cybersecurity. For cybersecurity international cooperation, Indonesia has become a Full
Member of the Asia Pacific and APCERT FIRST (Forum for Incident Response and Security Team) of the world. Indonesia also has become a Full Member and founder of the OIC-CERT (Organization of the Islamic Conference-CERT). International cooperation can also be interpreted in an effort to participate or agreed to an international agreement. Currently, Indonesia is trying to ratify European Union of Convention of Cybercrime. This Convention held on 23 November 2001 in Budapest, Hungary. The meeting intended to discuss thoroughly the threats facing the international world of cyberspace-related crimes. This convention has been agreed that the Convention on Cybercrime included in the European Treaty Series No. 185.

IV. CONCLUDING REMARKS

1) The increasing reliance on ICT technology will require a careful distribution of regulatory and supervisory powers between financial sector authorities and other state agencies. Without a clear legal framework, jurisdictional conflicts are inevitably bound to arise in many countries.

2) The public and private sectors must become partners in supporting the development of cyber-security knowledge, investing in innovative technology and sharing information.

3) Recent ICT growth in Indonesia gives impact on high cyber threats. The Indonesian government has tried to address that problem by issued policies and regulations, developed techniques and procedures, established organization security, improved capacity building and conducted international cooperation.

4) The rapid growth to global electronic crime and the complexity of its investigation requires a global presence. Presently, the measures are undertaken the banks are not sufficient and therefore it is imperative to increase cooperation among the banks across the world for the development of tools and models which can be applied to counter global banking cybercrimes.

5) Indonesia had many efforts to anticipate and protect cyberspace. This paper also proposes principles and strategies to improve national cybersecurity in Indonesia. Therefore, further work is to determine the ideal conditions for cybersecurity in Indonesia, furthermore by understanding the current conditions and the ideal conditions we can view the gaps that might be improved.

6) Cross-disciplinary and holistic cybersecurity research is needed to solve these new challenges. Due to the complexity of the field, research must meet the four basic paradigms of science: the theoretical, experimental, model-based and databased computational approaches.

REFERENCES

Accenture. 2015. Bridging the Technology Gap in Financial Services Boardrooms.

Asghari, H. 2010. Botnet mitigation and the role of ISPs: A quantitative study into the role and incentives of Internet Service Providers in combating botnet propagation and activity. The Delft University of Technology.


Sofia de Oliveira, Inês and Alexandra Stickings, 2016. Financial Institutions and Cybercrime: Threats, Challenges and Opportunities


