International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Is There Impact of Worst-Managed Corporate Governance on Cyber Attacks in Indonesian Biggest Banking Sector Organization: Literature Review Perspective (A Case Study at XYZtbk.)

Ach Maulidi

Sheffield Hallam University, Howard St, Sheffield S1 1WB, England, United Kingdom

Abstract: ***The aim of this study is to theoretically analyze impact of corporate governance on cyber attacks in Indonesia biggest banking sector organization. It is very interesting to study this matter, because Bank XYZ is broadly known asone of leading companies getting involved in financing system in Asia regions, but it is to be regular victim from outsider attackers. This study confirms that poor corporate governance is the presumably the main causes of cybercrime occurring in this bank. Security awareness and training are critical point to the success of a security implementation because they have strong influences on improving and maintaining security level. Such efforts need to be ongoing (well-rounded training programs), and they at least include understanding of policies, procedures and red flag (current threats) to both users and all employees. Raising awareness from users towards symptoms of intrusion probably can enhance prevention and enforcement. The more routine meeting taken place in this bank to communicate the issues related to the technical aspects of the system and networks, the more likely employees will internalize the fact that security is everybody's responsibility. It is also better if this bank hires outside trainers to provide education and training about special knowledge in relation to the methods, implementations, and capabilities of the systems used to manage security. If users especially IT department staffs have already obtained advanced knowledge regarding how to deal with phishing, how to identify symptoms of a virus infection and types of attack strategy to access to network, how to manage spam to avoid malicious viruses, how to make proper written rules/protocol for sophisticated firewall to circumvent software exploitation, the unexpected system behavior attacking this Bank can be terminated as soon as possible.***

Keywords: corporate governance, cyber-attacks, viruses, awareness, firewall

1. Introduction

The establishing concept of e-banking has already attracted great attention from business fraternity, as well as of researchers, scholars and investment communities across the world, due to today's sophisticated attacks to IT infrastructures. E-banking Technologies provide obvious advantages to consumers in terms of convenience to make routine banking exchanges beyond national boundaries and beyond office hours, but that growth of fascinating technologies also leave great fears of unlawful behaviors as long as the problems of ineffectiveness of telecommunication services and lack of adequate security systems still remain exist.

Realistically speaking, nowadays, cybercrimes are no longer isolated amateurs but they belong to well-structured organizations with clear motivation (money and goals). It is affirmatively evidenced by survey conducted by KPMG (2014), showing that organized crime motivated by money is the highest percentage from all of cyber-attack motivation with score 58%.The rising cybercrimes around the world have already given widespread fears and panic among Indonesian governments, security researchers, network manufacturers, business and investment communities and as well as societies. According to one of study conducted by Daka (2013), which is commissioned by British Embassy in Jakarta, found that Indonesian enterprises experienced 39 million attacks where 35% came from outside the country and 65% originated from within. Furthermore, based on Threat Exposure Rate (TER) in "The Security Threat Report 2013" from Sophos, because the number of cyber attacks against Indonesian enterprises continues to increase, Indonesia is considered as riskiest country in the world with the highest percentage of experiencing a malware attack, 23,54%.Therefore, dealing with the rapid growth of cyberspace in general and hacker acts in particular, in fast moving computer communication revolution in which every individual is likely to be affected, is the main challenge not only for the someone in the security department but for all of us.

2. An Overview of Indonesian's Corporate Governance

In relation to Indonesia capital market, Capital Market Supervisory Agency and Financial Institution (BAPEPAM) has the majority role in drafting, guiding, supervising capital market regulations, and it is a part of governments (Capital Market Law, 1995). BAPEPAM is not independent of the government's influence as it is a division of the Ministry of Finance and it should report directly to the Minister of Finance. As a consequence, this becomes huge dilemma for BAPEPAM to rule and implement its primary duties, because Indonesia government's position holds majority shareholders in all of the state-owned enterprises listed in Indonesia capital market. Indonesian stock exchange activities, therefore, may be injected by excessive government interventions. In other words, the stock exchanges in Indonesia seem to be controlled by the government.

Before going further to discuss Indonesia corporate governance model, it is very essential to explain critically privatization scene in Indonesia. Generally speaking, it will be accepted that the most pivotal result of privatization is a decisive commitment to increase effectiveness, productivity and efficiency in new privatized companies and, as many as possible, this effects have to generate worth outcomes to economy as whole. Alarmingly, the dominance of the rampant protectionist behavior of government through its privatization ideology will eventually result in serious problems in setting and implementing principles of effectiveness and efficiency, specifically in terms of maximizing enterprise's resources including funds collected from capital market. It is due to lack of adequate supervision mechanism from other enterprise's business colleagues and disproportionate power of majority shareholders (bureaucrats).

In addition, because of government as predominant shareholder (golden share) in listed state-owned enterprises (Daniel, 2003), it can be justified that this kind of privileged share may become proper bridges for government to appoint the member of the boards of directors and commissioners, while other stockholders cannot assign their representatives in both places. As substantial evidence demonstrated by a study was carried out by Well (2001) stating that Indonesia listed companies had approximately 80 per cent of foreign investors but in fact, they was not protected because of lack of sufficient surveillance and law enforcement. This concern affirmatively there are conflict of interest between minority shareholders and controlling shareholders that leads to negative disputes between the board directors, managements, and minority shareholders, and between major shareholders and the business colleagues of enterprise, and unequal access to information (*information asymmetry*) to all shareholders, and these concerns generate into long-term degradation or even bankruptcy. Therefore, it can be generalized that the intricate corporate governance mechanisms will not only affect the company itself but also it will affect a country's economic cycle, society, and as well as investment communities.

The recent Indonesia financial uncertainties in 2008 and mid-2013 have already given many lessons and highlighted the tremendous social and economic challenges facing Indonesia and countries across the world because Indonesia actively participates in prestigious world forums, for example World Economic Forum and G-20. As consequence, Indonesia governments under Indonesia finance ministry are seeking the most effective measures to deal with these increasing challenges and recognizing that private sector models can offer new innovative approaches to contribute to the emergence of social impact investment. The mechanisms of Indonesian corporate governance, in an era of increasing capital mobility and globalization, become a major concern for Indonesia central governments for improving competitiveness in world stages by reforming the backwardness of corporate governance regulation. Thus, it is clear that the role of enterprises is very important to build and maintain the condition of wellbeing for a cross-section of society and to operate government systems.

Even though, government of Indonesia put great efforts to establish good corporate culture in listed companies, the government does not realize conscientiously that the biggest serious problem, in terms of root causes of weak corporate governance system, is corruption rate that have already been rampant in all sectors. Corruption Eradication Commission (KPK) (2015) discovers the increasing number of fraudulent financial reporting due to the weakness of internal control system from 421 scandals to 1,634 scandals, and alarmingly those biggest scandals happened in corporate atmosphere. In 2014, based on a study conducted by Transparency International (TI), Indonesia corruption perception index, from 175 countries, placed at number 107. Unfortunately, it remains at number 6 associated with other ASEAN countries in associating with corruption index.

3. Why Indonesian Corporate Governance be Less Effective

Indonesian governments to promote good corporate governance in an era of emerging capital mobility and globalization try to rearrange corporate governance concept under finance ministry department. In 2004, Indonesian finance minister revised National Committee on Good Corporate Governance (KNKG) by issuing ministerial decree RI No. KEP-49/M.EKON/11/TAHUN 2004, to discuss the proper corporate governance concepts that are suitable for Indonesian enterprises circumstances. This institution gets aids from various departments and as well as House of people representatives. This section, thus, will critically analyze and discuss why Indonesian corporate governance code is still ineffective.

In this discussion, this paper will explore the effect of Indonesian culture on model of corporate governance by critically appraising the household relationship in Indonesian listed companies. This essay looks at family relationship because contemporary studies have succeeded to demonstrate that a large percentage of Indonesian economy operation rotates around enterprises organized by a particular cluster of wealthy and powerful family group. Therefore, these families' values and culture, indirectly, presumably influence on how Indonesia corporate governance works (runs).

The relevant laws regulating family relationship in Indonesia listed companies are Indonesia central bank regulation No.2/27/PBI/2000, documenting that "family relationship is prohibited from sitting on the board of commissioners'', and regulation C1 (a) of IDX for security registration I-A mentions that "a listed enterprise at least 30 % of its commissioners board must comprise of independent commissioners'' (IDX, 2001). To clarify 'independent commissioner' IDX also continues to state on C2 (a) and C2 (b) that "an individual must not has 'affiliation' with any other commissioner/director or the controlling shareholders". Unfortunately, in these regulations, there is no precise definition of affiliation.

As result of that concern, it can be concluded that those regulations succeed to regulate what should not occur however they miscarry to realize what truly occurring in the real circumstances is. An empirical study carried out by

Tabalujan (2002), found that there were 125 companies from the total number of 307 listed companies, in 2001, which had the number of household members in their committees. According to fraud triangle theory, an individual or organization is easily to misrepresent information disclosure that should be disseminated to the stakeholders if he has a perceived opportunity to make unethical agreements (Albreacht et al., 2012).

Therefore, the likelihood of potential wrongdoing risks among companies that have the relationship of family members in their boards are greater than others have not, because their further decisions in relation to their business activities could be influenced by family deliberations around the eating room at home as many as by official meetings are conducted around the board room at work. Based on a study carried out by The Asian Development Bank and Jakarta Stock Exchange (2003), only 8 enterprises or 3, 12 per cent have already implemented corporate governance standards. Therefore, it can be assumed that the level of compliance of the corporate governance code, in Indonesia, remains ineffective. There is an inclination for Indonesians to prefer to circumvent any code aiming to obtain material advantages for themselves, and this unethical act becomes concrete obstacles for the implementation of good corporate governance.

Furthermore, information asymmetry theory, in current literatures, views that a firm's asymmetric Information has crucial negative consequences of the mechanism of corporation model. One of temporary studies carried out by Cai et al., (2009), documents that the mechanism of corporate accountability level depends on the level of firm's asymmetric information environments. Thus, there is no doubt to argue that Indonesian corporate systems especially accountability aspect, is still questionable if we look at sophisticated Indonesian corporate culture scene that has strong family relationship in board of directors. As concrete example evidenced by an empirical academic study conducted by Daniel (2003), stating that one of the biggest problem in Indonesian listed companies is healthiness of financial structure condition.

Apart from that, Indonesia has a unique agreement culture that is promoted by political situation. The majority big corporations in Indonesia are owned by an individual sitting on higher positions in strategic Indonesia parliaments and institutions playing large role for Indonesia affairs. The political connections between government and entrepreneur are proper bridges to acquire access in terms of unscrupulous cooperation process among them. This issue obviously mobilizes worse situations in relation to stability, fluidity, social mobility and economic mechanisms through creating and imposing fallacy regulations that lead to emerging other problems because they do not be created on behalf of public interest. This phenomenon strongly matches with political theory, stating that potential issues will fail to be addressed if an imbalance portion of political business motivated by self-interests does take place in that discussion (Howes, 2005), and it doubtless will be generally inclined to commit intentional conspiracy aimed to mislead other parties with irrespective of the merits of the case.

Even though, there are many different independent institutions that get involved in setting up and supervising the implementation of corporate governance code, it will not change too much if enormous power (interventions) from particular parties still exist on revising corporate governance framework. Basically, the competitiveness and ultimate success of listed companies is the impact of perfect cooperation from various stakeholders such as customers, distributors, creditors, employees, suppliers, investors and as well as governments with their good regulations. Apart from that, Indonesia has many regulations disseminated to public that can trigger to overlapping rules (ineffective regulations), and it as major factor leading to poor corporate governance in Indonesia.

Therefore, the tentative summary for this section is that Indonesia has a lot of regulations and legal institutions, but the existing Indonesian need is an appropriate changed legal culture that is designed to be used in competitive market atmosphere. In other words, Indonesian corporate situation does not need more law, but less with precise regulation to deal with current concerns. Furthermore, there are defective efforts in improving Indonesian corporate governance regulation. Even though Indonesia establishes new laws, and institutions, it does not mean, it will enhance the effectiveness of setting up and implementing corporate governance code as long as there is no awareness of the inherent consequences created by emerging them.

4. Research Method

This research adopted a case study approach to take advantage of rich information and analysis, and to provide an in-depth elucidation of it.The researchers will concern to the unique of features of the case. In order to give a representative review of works, a literature search was conducted to identify influential papers. The central issue of concern is the quality of the theoretical reasoning in which the case study researcher engages. The researchers will identify what is the main root cause of cyber attacks that occur in the chosen banking sector, and then, we will consider what is unique and what is the common across cases, that frequently promotes theoretical reflection on the findings. The focus of this study is on the cases and the unique contexts by relying on theoretical framework. In order to conduct a review of influential papers, a literature survey was done. The researchers identified the most prominent articles that discuss cyber crimes in banking sector organizations and corporate governance, especially in Indonesia contexts. For literature search, we used ISI Web of Science, Emerald text, Science Direct and Inderscience which we consider provide sufficient information on articles in leading scholarly journals in the area.

5. Background of the Study

This study anonymously employed one of the biggest banking sector owned by Indonesian government(State-Owned Enterprises; BUMN) which is always hijacked on continuous basis. The name of chosen original bank switched intentionally into Bank XYZ tbk.

In transparency aspect, the Bank XYZ's commitment as mentioned in its CGC report cites:
"The Bank discloses information that includes but is not limited to the vision, mission, business objectives, strategy, financial and non-financial conditions, structure of the Board of Directors (BOD) and the Board of Commissioners (BOC), controlling shareholders, risk management, internal monitoring and control system, implementation of compliance function, GCG system and implementation, as well as material information and fact that may affect investors' decision".

And,
"The Bank discloses information in a timely, adequate, clear, accurate and comparable manner, as well as makes it accessible to the concerned parties (the stakeholders)".

However, in 2005 this bank in practical sides, according to documents cited by the Financial Times, did not touch its CGC principles. In other words, this bank had a bribery case with more than 30 companies which had relationships with this bank. Senior officials of this bank colluded with those corporate clients. Separately, one of national newspapers posted in 2008, mentioned that there many commentators from different level of backgrounds arguing that " …this bank becomes a suitable target for hackers because of a lack of effective communication and coordination between center bank and branches of bank, unprofessional treatments towards customers and imbalance budget resources for IT development…"
Whereas, in its CGC principles states that;

"The Bank adheres to the principles of prudential banking practices and guarantees compliance with the applicable regulations"
and,
"The Bank applies check & balance system in conducting its management".

Along with the concern of fraudulent activities, it is very important to discuss its board composition and remuneration system that are presumably and indirectly the primary root cause of cyber attacks faced by Bank XYZ.

Analyzing board composition
Generally, a company's success and long-term survival is dependent on board's decisions in terms of facing a wide range of new challenges and establishing the long-term vision and strategy for the company (Mishra, 2013). Board diversity causes a business to be more profitable and creates values for shareholders (Faleye, 2007). That line statement substantially and practically evidenced by board composition in Bank XYZ, where that company emphasizes on board diversity in terms of gender and in the wide arrange of relevant backgrounds, races and nationalities. They believe that diversity, in all aspects, is important in order for a board to operate effectively according to its annual report 2015.

It is clear that this Bank XYZ may make more astute decisions in the complexities of the environment because a wide range of voices drawing on various life experiences can be represented. Evidence suggested that enterprises with a more women representation at top management and boardroom levels will run optimal that those without (McKinsey&Company, 20010) and gender-diverse boards will contribute a positive consequence of economic performance (Carter et al., 2003; and McKinsey&Company, 2010).

However, it is still reasonable to argue that a firm with strong gender-diverse boards may witness more conflict and disagreement causing long and drawn-out deliberations—a big concern when that firm requires to react quickly to make market shocks. There can also lead to ineffective communication if the boards of the firm are reluctant to share crucial data/ information with demographically divergent directors. One of studies suggested that having a higher proportion of women on US boards have a negative consequence for the ratio of a company's market value to the replacement value of the firm's book equity and its return on assets (Smith et al., 2006). It also parallels with Shraden et al., (1997) and Zahra and Stanton, (1988), found that the percentage of women on the board statistically have a significant negative impact on firm's values.

Furthermore, another point is the diverse range of nationalities represented at board composition. That point will impact on an increased on a diverse boardroom that might result in more diverse opinion, miscommunications and more conflicts of interest triggering negatively to the board performance. One of recent studies suggested that board diversity affects negatively company's values (Carter et al, 2010). Furthermore, according to the similarity-attraction theory, the notion of diversity will fight against firm performance because individuals are more likely to interact with others who have similar backgrounds, believes and historical events (private lives). Thus, there might diverge interests (agent problems) because the synthesis of a large number of traits in the boardroom is likely difficult.

Analyzing remuneration system
In this Bank, why executive's remuneration figure is always higher that chairman and non-executive one as presented in its annual report, and how that remuneration package is determined, is it measured by pure performance/ achievement financially or other things. In practice, most board members engage in both advising and monitoring. Of course, director's pay packages are determined by remuneration committees, but affirmatively, it has an impact on the persons who are being paid, and, obviously this context will lead to agent problem/dilemma. Some evidence suggested that the relationship between director/executive pays and company performance is often tenuous (Murphy, 1999), because social, psychological, and political factors are likely involved in determining executive compensation (Devers et al, 2007).

This is surprising in view of the fact that labor costs, in this company, are considered costs which are having significant impact on reducing firm's profit, with more than half of total costs, while in another condition shareholders need high returns from their invested money. Jensen and Meckling (1976), claimed that remuneration contract, in the agency theory framework, is one of ways to ensure that directors act in the shareholders' interests, but many scientists have

proved that remuneration packages intended to encourage executive to act in shareholder's interests frequently fail (Patton, 1972).For example in remuneration report 2015, how can shareholders measure short and long-terms incentives for executives have been appropriate for their (shareholders) interests?, if they did not justify why executive pay packages substantially increase from previous year, and the chairman's remuneration figure is not disclosed in that report. In this concern, therefore, the executive's remuneration figures are being a skeptical thing in corporate governance scene if there is no adequate justification. In other words, executive remuneration seems closely associated with psychological factors and CEO power than firm performance.

This paper, because of thoseplausible concerns, assumes that it is very reasonable if Bank XYZ becomes suitable attacks from both organizational insider and outsider attacks on continuous basis. In addition, as long as there is no adequate internal management system or robust corporate governance, internal security of electronic organization to safeguard sensitive information will be still weak. This paper takes Bank XYZ tbk as main discussion since this bank is the biggest state-owned banking sector organization and Indonesia itself is a major shareholding in this bank (IDX, 2016). Thus, the major implications of this paper is to give significant contribution to Indonesian banking sector organizations in general and bank XYZ tbk in specific in terms of fighting against cybercrime, and to deliver knowledge andinsight to users and academic environment in relation to preventing those exclusive criminal syndicates and an additional reference for further academic studies.In the further discussion will elucidate and analyze cybercrime in Bank XYZ organization before linking it with corporate governance, because it very important to know the modus operandi of this kind of crime.

6. Analysis of Cybercrime in Bank XYZ Organization

This section will critically discuss and analyze why and how attacker fraudsters in those cases become successful to commit their unlawful activities.

Vulnerability – The security deficiencies of the system in Bank XYZtbk

Undoubtedly, authentication mechanisms, in internal security of electronic organization, are considered as the critical security element to reduce high-risk transactions and to safeguard sensitive information including the movement of funds to other parties (Bishop, 2005). If this authentication process is hacked by Trojan virus attack or a complex credentials theft, the bank has no way to distinguish between legitimate and illegitimate clients. Recently, to enable the clients of Bank XYZ tbk to commit monetary transaction through internet network during 24 hours require employing hardware token or using mobile device as valid token via SMS.

In theory, two-factor authentication scheme like Token device perfectly can protect worth information because it meets three fundamental elements, such as time synchronous, event synchronous and challenge-response, to fight against various attacks (Vacca, 2013). In practice, on the other hand, Trojan horse can defeat this sophisticated approach started from login time. In order to know the token's characteristics, user has to import token's serial number into the authentication server, when user logs onto network, she in her email faces with some challenges that must be answered by her assigned token (Vacca, 2013). Because a token is assigned to user by linking its serial number to user's record stored in the system database, more pernicious forms of malware can intercept that network traffic to capture a file containing that information and change it silently (Matthew, 2005).

Furthermore, after user, during transfer process, have already provided the Bank with sensitive data (valid One Time Password (OTP) from his matrix card), Trojan can modifies the user-entered destination bank account to other of its election and permits that transfer process to proceed as planned (Claussen, 2008). At same time, Trojan reveals information confirmation to user that transfer succeeded perfectly (Claussen, 2008). Therefore, it is reasonable to argue that because of the security deficiencies of the system in Bank XYZ tbk, Trojan enables to gain unauthorized access to user's workstation. It is substantially evidenced by contemporary studies. Andrew (2007), noted that one-time passwords has its own threat, even though it relies heavily on two-factor authentication, the window of chances for attackers still remains higher, so obtaining one-time value is not enough. Similarly, Kim et al (2009), also documented that one-time authentication scheme is still insecure under an impersonation attack, a replay attack, and modification attack, in which hacker can interrupt the authentication scheme without intercepting any transmitted data.

A part from that, another important point that allows attackers to perpetrate their wrongdoing successfully in this Bank is the providing OTP with SMS. According to author's experience discussing it with one of experienced Indonesian National Banks employees and some academic studies, this kind of service is considered as vulnerable authentication server because many banks create a random code through the Web channel to confirm the operation and send OTP to the user's mobile phone (Biryukow et al., 2001; Hamdare et al, 2014). In other words, these authentication service mechanisms heavily depend on security offered by the cellular web operator. To prove whether OTP conveyed by SMS messages is secure. Mulliner et al., (2013), examined two main areas such as the infrastructure of mobile phone and the design of phone cellular as well as the software and hardware for smartphone. According to their analysis, they argued that the judgment of SMS containing in good reliability to transport OTP is not true anymore.

Because technology of GSM lacks mutual authentication and adequate encryption algorithms (Mulliner et al., 2013), and the femtocells can be abused to intercept 3G communication, including SMS messages (Biryukow et al., 2001), mobile phone malware (Trojan) can easily intercept that cellular network traffic to capture SMS messages containing a verification code transmitted over-the-air and silently change that token's serial number (Mulliner et al., 2013; Biryukow et al., 2001; Steve, 2012). As consequence, phisers can exploit those sensitive information for capital

gain through infecting mobile malware without the knowledge of users.

SMS OTP as a method of online transaction safeguard is not difficult to hack (Hamdare et al, 2014; Nilanjan and Ramkrishna, 2013). Infection techniques are mostly used to deceive users namely Repackaging, Update Attacks, Brower Attacks, Malvertizing (McAfee, 2011). Steve (2012), Documented that approximately 1,074 (80%) of the Android problems are caused by poor programming practices or poor authorization and authentication that trigger to vulnerable data. Therefore, there is no doubt to argue that prevention of network intrusion adopted by Bank XYZ tbk is still vulnerable to be attacked due to insufficient antivirus program that cannot mitigate confidential information stealing malware even though this Bank supervises every transaction.

Vulnerability – Data accessible from anywhere
To be productive for business' affairs, Bank XYZ tbk allows their employees and clients to access data/information from anywhere using a variety of technology devices. In this situation if the IT department is incapable of managing server authentication/online file storage sites as well as its plans, fraudsters will indiscriminately exploit this vulnerabilities and bank will experience few impediments as soon as possible. From this lack of understanding of how some of these online databases are generated, the likelihood of denial-of-service (DoS) attacks will take place by spreading malicious software that try to interrupt or even disable authorized user's access to bank's network and system.

In the contemporary internal network security systems possessed by Bank XYZ tbk are Personal Identification Number (PIN), Secure Sockets Layer (SSL), and Firewall. In existing theories and literatures, these kinds of network security systems, if cannot managed well, are very vulnerable to be exploited/ hijacked by attackers (Bhope, 2012; Vacca, 2013; Gupta et al, 2012). Basically, sensitive information, including password and PIN, are routinely transmitted over the network and Bhope, (2012) from his study claimed that performance of SSL sometimes cannot balance server authentication in relation to the distribution of the work load among the client and the server due to a large amount of traffic.

In other words, attacker can benefit from the deficiencies of SSL by deploying denial-of-service (DoS) attacks with generating too many handshake requests to exhaust the source of the targeted organization server without the need to be validated by the network (Sukalp, 2012). Therefore, If DoS attacks successfully make an online service unavailable to intended legitimate users due to unmanageable the sudden increase in demand of its service from the clients, unexpected user will access, abuse and exploit to resources. As one of results from this unexpected system behavior, by using the harvested personal information, attacker can make deceitful credit-card charge and apply for credit in the victim's name.

In 2008, Bank XYZ tbk collectively suffered from USD 1,2 billion to repair its internal network security systems due to external threats (JawaPoss, 2009). It means that firewall possessed by Bank XYZ tbk needs more intention in terms of future investment for well improvement when sensitive information and documents are concerned with a much wider domain and the business transactions are really heavily based on technology. Even though firewall is one of network security systems that can allow and block incoming and outgoing traffic, it does not mean that it can guarantee to protect internal network from external malicious intrusions (Rescorla, 2001; Parmar and Gosai, 2015). Because the effectiveness of a firewall depends on its rules (Bishop, 2005), appropriate written rules play an important role of the successful of implementing a firewall. Properly written rules, therefore, requires sophisticated knowledge of network protocols supplemented by well-rounded training programs to minimize improperly configuration due to neglect or lack of training from the staffs of IT department.

Therefore, because of data accessible from anywhere, it ultimately generates to the imbalance process in the workload, and this is presumably the main root cause of the DoS attacks in Bank XYZ tbk.

7. Main Discussion and Conclusion

According to the plausible analyses above, it can be concluded that the fundamental root cause of vulnerabilities in Bank XYZ tbk is ineffective corporate governance corporate policies and poor management systems. Because of those aspects, this bank is recently heavy relying on Personal Identification Number (PIN), Secure Sockets Layer (SSL), and Firewall to secure its network traffics. On the other hand, many contemporary studies documented that those security products could be still exploited by unauthorized users by spreading malicious malware or deploying Denial-of service (DoS) attack.

Alarmingly this bank is classified into the biggest net income compared with the top state-owned banks that are listed in Indonesia Stock Exchange (http://www.idx.co.id/index-En.html) but this bank cannot afford to purchase other sophisticated security infrastructures to safeguard its sensitive information/ data which are routinely transmitted over the network. This concern is presumably caused by ineffective management system especially in terms of IT investment. In addition, another strong assumption of imbalance budget resources for IT improvement is caused by fraudulent act conducted by one of managers in this bank.

Furthermore, another vulnerability triggered by ineffective security management system is related to the providing OTP with SMS. This service becomes great challenge for managers of IT department to secure credibility of token's serial number from more pernicious forms of malware. The main reasons for this issue, in today's sophisticated attacks, are that managers lack knowledge of fundamentals of information technology and IT professionals in this bank lack understanding of technical IT infrastructure frameworks. Because of those reasons, the volume of threats to network may become bigger as long as this bank does not take into account the security training programs for both parties. There are so many things that can go wrong with

network traffics security if this bank fail in having solid control of over security monitoring, administration, and implementation. This phenomenon affirmatively can result in a security nightmare for this bank and ultimately leads to loss of reputation and great financial cost.

Despite the enormous influence of ineffective security management to safeguard its sensitive information, managements of Bank XYZ on corporate governance system still remains problematic. Even though the pioneering efforts distributed to understanding goals incongruence among principals and agents as a function of contractual relationships set up within the Bank, the subsequent corporate governance participants failed to fully play in ensuring better governance and risk management practices. Managements of this bank need to encourage a broad-based risk management culture that traverses traditional organization boundaries. Because this bank witnessed corrupted activities that are presumably the main cause of cyber attracts, boards need to be encouraged to a broad-based view of their responsibilities, that includes a detailed understanding of the risk management of the business; in essence, the have to understand the totally of their role.

It is not a simple matter. The turbulence in botha much wider domain and the business transactions that are really heavily based on technology, and inadequate corporate governance have raised many questions over the governance of organizations and more importantly how risk management aligns with broader governance principles. It is very important to underline that the unhealthy financial and management systems might trigger to other consequences, namely the purchasing and implementation of sophisticated security products and budgeting education and training programs. Those aspects play an important role of mitigating the risk of illegitimate exploitation of bank's network and information assets. Generally speaking, even though an organization can afford to purchase sophisticated secure infrastructures, namely Firewall, Antivirus Programs, and Intrusion Detection Systems, they will not work well if there is no supportive workplace atmosphere and a lack of adequate controlling other IT operation and security mechanisms to support those products. It is strongly evidenced by a study carried out by Ponemon Institute in 2015, stating that improperly managing IT operation, education of staffs and security priorities are the main cause of more than two-thirds of banks in U.S. suffered from DDoS (Financial Times, 2013).

This bank cannot add other security infrastructures to secure its network traffic from today's sophisticated attacks, and it just heavily relies on previously deployed traditional technology as discussed in previous vulnerabilities. It is important to reemphasize that firewall does not have the intelligence or reporting capabilities to monitor the entire network (Dulaney, 2011). Keep in mind that all of this bank's efforts will be wasted if this enterprise does not struggle vigorously and seriously to take into account an employee's inherent trusting nature and its risk internal management system. It is reasonable to argue that human weakness (greed) will push to exploit the system vulnerabilities to obtain capital gain. It is substantially demonstrated by an empirical academic study conducted by Al-Saggaf et al. (2015), stating that greed factor triggered unethical conducts in the Australian Information and Communications Technology (ICT). In this point, therefore, the primary root cause of the propagation of outside malicious code/malware attacking this bank is ineffective corporate policies that lead to the abusing and embezzling a company's tangible asset.

Without doubt, another potential likelihood of attack in this bank, as long as ineffective corporate policies and poor security management are addressed immediately, is impersonation (stealing access rights of legitimate users) committed by an inside employee.Kovacich and Jones (2005) argue that cybercrime may be perpetrated by organizational insiders or outsiders. Expert agree, however, that the catastrophic threat comes from disgruntle workers (insiders), regardless level of positions in that company, who are authorized to access the company's computer system (Bishop, 2005). If insider threats (misuse of authorized privileges) do take place in this bank, they will become the most hazardous threat and a very complicated concern to solve because they typically have already known the firm's security system weaknesses, and often known enough passwords to bypass many security controls. Those unauthorized users, therefore, can masquerade as the authorized ones with significantly less probability of detection to perpetrate morally unjustifiable acts. Moreover, when the internal computer security mechanism deteriorates, the quality of information flow policy become ineffective, discretionary access controls are not well managed and its corporate governance weakens, it cannot be denied again that the opportunity of committing fraudulent activities will appear in the surface of company immediately.

In addition, those exclusive activities of criminal syndicates occur successfully due to moral justification from perpetrators with low empathy on damages caused by their harmful acts related to the insidious nature of computer piracy. This effectively and directly enables their ideology and rationalization to legitimate wrongdoing or violence as divine ordination without any feelings of righteousness. In this case, greed and acquisitiveness from organizational insider threat may arise due to powerful belief that firm should pay for perceived inequities. That is concretely evidenced by one of academic empirical researches conducted by Murphy and Dacin (2011), documenting that rationalization is a human mechanism process that allows individuals to justify immoral manner to commit fraudulent actions. Therefore, the proliferation of computer-related business activities has significantly aggrandized the criminal behavior especially computer crime (hacking) as long as there is no serious monitoring and evaluation of the effectiveness of corporate governance principles.

Because impact of poor corporate governance regime, in this Bank, which result in unethical conducts, separating the executives' and non-executives' roles on the board has a crucial role in enhancing the monitoring of management activities.The audit committee in this Bank should be chaired by a non-executive director and is ultimate anti-fraud committee thathas responsibilities and authorities to ask all internal information and encourages employees to contact them if there is any suspicious act at work.

Additionally, the audit committee is to ensure that the management provides sufficient and thoughtful information about all corporate activities to regulatory authorities and shareholders. Associated with the cases occurred in Bank XYZ, we notice that multiple roles might give rise to conflict and ambiguity towards business' objectives. The difficulty of organizing this could well lead the central management of this bank to leave its operational managers to concentrate on carrying out their specific responsibilities. Analytically, it is equally clear that it is wise always to look at the activities of managers across the organization in terms of the relationship of these activities to the organization's strategic direction.Thus, the symptoms of things going wrong or fraudulent activities as a result of multiple roles in the workplace will be successfully pressed.

In the absence of effective mechanism to operate bank's activities, the high level of worker commitment towards a managerially conceived corporate direction that is implicit in the notions of strategic intent and of the learning organization is something that organization frequently aspires to and many try to bring about. We believe that, in the shareholders points of view, CEO will make every effort to work cooperatively with its subordinates intended to achieve the goal of sustainable wealth maximization in cost-effective procedures and to highlight deficiencies.Unfortunately in relation to those concerns, there is no specific protection plan available defining and regulating what must be implemented to safeguard the an organization's tangible and intangible assets but this essay suggests some appropriate preventive measures to tackle and protect assets including information associated with this bank as discussed below.

Regulating and applying effective policies

Today's enterprises are eager to grasp the notion of applying sophisticated technological control systems to safeguard the sensitive data held in their computer systems but this effort, in large enterprises like Bank XYZ tbk, will be less effective, if there is no an adequate security policy. There is no doubt to argue that the strength of an enterprise's system security mechanism is determined by the details in its policy security. Thus, it is very essential to establish a policy team consisting of at least one member from the IT department, the employees on the frontline, legal, and senior administrators to deliberate the prioritized recommendations for eliminating or mitigating the vulnerabilities. A clear understanding of the structures of responsibility and authority stated in the policy helps in carrying out security management and provides a strategic instruction to various initiatives and maintains the high-integrity data flow. Therefore, an ideal security policy must clearly define the scopes of responsibility for users, administrators, and managements (clear segregation of duties), inform the step-by-step directions on how to accomplish a specific task in a specific manner, precisely describe a clear vision of a secure environment to make all employees, regardless of position level in that organization, aware of information security threats, be consistently implemented throughout the employees without any tolerable condition for violating the rules, and administer daily supervision and control to reduce myriad operational problems.

Establishing a culture of security

One of the biggest security assets owned by an enterprise is its employees, but only if they have already understood and made commitment to comply with security policies ruled in that enterprise. Specifically in Bank XYZ tbk, it will be helpful if level of managements want to study some critical professional business concepts that are followed by taking one step forward to study fundamentals of IT professional and Information technology. Studying those concepts is very beneficial to this bank in relation to budget resources for development of IT infrastructures, and they can enhance the employees' productivity especially focused on the security issues. The most important aspect in this point is the encouragements of employees to respond as soon as possible to confront strangers towards their both tangible and intangible assets. To do this, monetary incentives or promotion are considered as one of the best possible approaches that should be prioritized by management.

Applying effective communication and information

This section relates to the flow of information in two directions in both internal and external bank including branches of bank. This information flow mechanism, however, is concerned with all information, not just up or down. To address vulnerabilities attracted unethical behaviors as mentioned above, this bank should make sure carefully that information flowing downward to the line functions should be accurate and precise in order to produce the fascinated result as expected, and information related to employees' performance should flow upward through bank's management by providing objective feedback conveyed by formal and informal mechanisms. A part from that this bank should encourage employees to feel empowered in terms of raising concerns, reporting those concerns and suggesting measures to deal with those concerns aiming at enhancing quality of process. Cendrowski et al, (2007) documented that an open communication in an organization is one of hallmarks of proper control environment.

This main activity at this point is for the team to carefully review all the information and processes that are attempted to be exploited. To do this, before the review and analysis steps start, the team established by the high authority of this bank, in the processing step, should determine scope and objectives of the review and cull the volume of information because reviewing each and every piece of documentation may very well be infeasible. After conducting review, all discoveries are analyzed to identify any suspicious strangers and eliminate any false positives and decide the proper preventive efforts.

Applying penalty and incentive programs

In information security context, it is strongly needed by organization to enforce penalty and incentive mechanisms as deterrence action to perpetrate undesirable behaviors within organizations. In IT context, Straub (1990) from his study documented that deterrence measures are an important program for minimizing computer abuse. Similarly, Herath and Rao (2009) and Peace et al., (2003), noted that perceived threat of punishment affect positively the level of unlawful acts reduction in the firms. In consideration of severity of punishment, therefore, if the level of punishment increases, an employee to violate the organizational policies

intentionally (committing wrongdoing) is likely to decline. From incentive perspective, on the other hand, many researchers have already carried out empirical studies in analyzing the importance of incentive mechanisms associated with moral motivation in analytical model (Brekke et al, 2003; Murdock, 2002; Benabou and Tirole, 2003). They argued that incentive mechanisms applied by an organization play an important role in encouraging desired behaviors especially in complying corporate policies, and information security procedures. Because employees seldom comply organizational policies due to inability to supervise employee behaviors (Herath and Rao, 2009), there is no doubt to argue that encouragement of desired behavior through penalty and incentive mechanisms is very useful measures for organization to reduce unethical conducts and enhance productive environment.

8. Acknowledgement

The author is indebted to the LPDP for financing my study at Sheffield Hallam University. Furthermore, the author appreciates the helpful comments and suggestions ofNaomi GrytaGhossany, working atquality assurance department of BTPN Syari'ah, Indonesia and then the author wishes to thank there reviewers of an earlier version of this paper for their helpful comments, Namely AbdulsalamBinomran, (Business school, Sheffield Hallam University), Ali Alnajar (Business school department, Tripoli University), and Mohammed (Advanced computer networks, Sheffield Hallam university).

References

[1] Andrew, L. (2007)*Time versus Event Based One-Time Passwords: E token*, Petach Tikva: Aladdin Knowledge Systems Ltd.
[2] Albrecht, W.S., Albrecht, C.O., Albrecht,C.C., Zimbelman, M.F. (2012)*Fraud Examination*. Boston, Cengage Learning.
[3] Al-saggaf, Y., Burmeister, O., Weckert, J. (2015). Reasons behind unethical behaviour in the Australian ICT workplace. *Journal of Information, Communication and Ethics in Society*, 13 (3/4), 235 – 255.
[4] Benabou, R., and Tirole, J. (2003) Intrinsicand extrinsicmotivation, *Review of Economic Studies*,70,489–520.
[5] Bishop, M. (2005*). Introduction to computer security*. Massachusetts: Addison Wasley.
[6] Biryukov, A., Shamir, A., Wagner, D. (2001)Real time cryptanalysis of A5/1 on a PC.Springer, Heidelberg, 1978, 1–18.
[7] Brekke, K.A., Kverndokk, S., and Nyborg, K. (2003) An economic model of moral motivation, *Journal of Public Economics*, 87 (9),1967-1983.
[8] Cai, J., Liu, Y., and Qian, Y. (2009) Information Asymmetry and Corporate Governance, *Journal of Accounting and Economics*, 47, 208-225.
[9] Capital Market Law, (1995). Republic of Indonesia Nomber 8/1995. [online]. http://www.sampoerna.com/id_id/investor_information/capital_market_regulation/documents/uu%20no%208%20tahun%201995%20tentang%20pasar%20modal.pdf
[10] Carter, D.A., Simkins, B.J., Simpson, W.G. (2003)Corporate governance, board diversity, and firm value. *Financial Review*, 38 (1), 33-53.
[11] Carter, D.A., D'souza, Simkins, B.J and Simpson, W.G. (2010) The gender and ethnic diversity of US boards and board comittes and firm financial performance. *Corporate Governance: An international Review* ,18 (5), 396-414.
[12] Cendrowski, H., Martin, J.P., Petro,LW. (2007) *Hanbook of fraud deterrence*, Canada: John Wiley & Sons, Inc.
[13] Claussen, H., Ho, L.T.W., and SAMUEL, L.G. (2008) An overview of the femtocell concept. Bell Labs Technical Journal, 13 (1),221–245.
[14] Daniel, W.E.(2003) Corporate Governance in Indonesian Listed Companies - A Problem of Legal Transplant. *Bond Law Review: Comparative corporate governance*, 15 (1), 345-375.
[15] Daka (2013) Meeting the cyber security challenge in Indonesia: an analysis of threats and responses [online] available at http://dakaadvisory.com/wp-content/uploads/DAKA-Indonesia-cyber-security-2013-web-version.pdf
[16] Devers. C.E., Cannella, A.A., Reilly, G.P., Yoder, M.E. (2007) Executive compensation: a multidisciplinary review of recent developments. *Journal of Management*, 33(6), 1016–1072.
[17] Dulaney, E. (2011) *Security: Deluxe study guide*, 2sd edition, Canada: Wiley Publishing, Inc.
[18] Faleye, O., (2007) Classified boards, firm value, and managerial entrenchment. *Journal of Financial Economics* 83 (2), 501-529.
[19] Gupta, A ., Seung-Hyun, S., Asmaa, M.S., Elisa, B., and Kangbin, Y. (2014). Detecting mobile malware threats to homeland security through static analysis, *Journal of Network and Computer Applications*, 38 (2014), 43–53.
[20] Hamdare, S., Varsha, N., and Jayashri, M. (2014) Securing SMS based one- time password technique from man in the middle attack, *International Journal of Innovative Technology and Exploring Engineering*, 11 (3), 154-158.
[21] Herath, T., and Rao, H.R. (2009) Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness, Decision Support Systems 47(2), 154–165.
[22] Howes, M. (2005) *Politics and environment: risk and the role of government and industry*. London: Earthscan.
[23] Jensen, M.C., and Meckling, W.H. (1976) Theory of the Firm: Managerial Behaviour, Agency Costs and Ownership Structure, *Journal of Financial Economics*, 3 (4),305–360.
[24] Kovacich, G.L., and Jones, A. (2005)*High-technology crime investigator's handbook*, 2sd edition. United Kingdom: Elsevier Inc.
[25] KPMG (2014). Forensic technology service: Cybercrime survey report 2014, available at, https://www.kpmg.com/IN/en/IssuesAndInsights/ArticlesPublications/Documents/KPMG_Cyber_Crime_survey_report_2014.pdf.
[26] Kim, M., Byunghee, L., Seungjoo K., and Dongho, W. (2009) Weaknesses and improvements of a One-time Password authentication scheme, *International Journal*

of Future Generation Communication and Networking, 2(4),29-38.
[27] KomisiPemberantasKorupsi (KPK) (2015)Laporan tahunan[online]. http://www.kpk.go.id/id
[28] (Corruption Eradication Commission (2015).Annual Report).
[29] Matthew, P. (2005) Evolutionary trends in bank customer-targeted malware. *Network Security*, 2005 (10), 4–7.
[30] McAfee (2011) Threats report: second quarter 2011.
[31] McKinsey&Company (2010) Women at the top of corporations: making it happen.
[32] Mirsha, R.K. (2013). Diversity and the Effective Corporate Board, Langford Lane: Elsevier Inc.
[33] Mulliner, C., Borgaonkar, R., Stewin P.,and Jean-Pierre, S.(2013) SMS-Based One-Time Passwords: Attacks and Defense. Springer-Verlag Berlin Heidelberg, 150–159.
[34] Murdock, K. (2002). Intrinsic motivation and optimal incentive contracts, *Rand Journal ofEconomics*, 33 (4),650-671
[35] Murphy K. (1999). Executive compensation. In *Handbook of Labor Economics (Handbooks in Economics)* (Volume 3a), Ashenfelter O, Card D (eds). ElsevierScience: Amsterdam, The Netherlands; 2485–2563.
[36] Nilanjan, D., and Ramkrishna D. (2013) An Approach of Secured Ecommerce Transaction Model without Using Credit or Debit Card, *International Journal of Innovative Technology and Exploring Engineering*, 2, (6),135-148.
[37] Parmar, H., and Gosai, A. (2015) Analysis and study of network security at transport layer, *International Journal of Computer Applications*, 121 (13),35-40.
[38] Patton, A (1972). Why incentive plans fail, *Harvard Business Review*, 50 (3),58-66.
[39] Peace, A.G., Galletta, D., and Thong, J. (2003) Software piracy in the workplace: a model and empirical test, *Journal of Management Information Systems*, 20 (1),153-177.
[40] Rescorla, E. (2001)*SSL and TLS: Designing and Building Secure Systems*, Boston: Addison-Wesley Longman Publishing Co., Inc.,
[41] Sophos (2013). Security threat report 2013. [online] available at https://www.sophos.com/en-us/medialibrary/PDFs/other/sophossecuritythreatreport2013.pdf
[42] Smith, N.V., Smith, V., and Verner, M. (2006)Do women in top management affect firm performance? A panel study of 2,500 Danish firms. *International Journal of Productivity and PerformanceManagement*, 55 (7), 569–593.
[43] Steve, M.D. (2012) Android malware and mitigations; Network Security. Elsevier, 2012 (11),12-20.
[44] Straub, D.(1990) Effective IS security: an empirical study, Information Systems Research, 1 (3),255-276.
[45] Sukalp, B. (2012). Server based DoS vulnerabilities in SSL/TLS Protocols, Master Thesis, Eindhoven University of Technology.
[46] Tabalujan, B.S. (2002) Why Indonesian Corporate Governance Failed – Conjectures Concerning Legal Culture, *Columbia Journal of Asia Law*. 15 (2),141-171.
[47] Transparency International (2015). [online]. Indonesia Corruption Index; Corruption by country/territory. [online]. https://www.transparency.org/country/.
[48] Wells, S. (2001) Moving toward transperancy: capital market in Indonesia.[online] https://aric.adb.org/pdf/aem/external/financial_market/Indonesia/indo_cap.pdf.
[49] Vacca, JR (2013). *Computer and information security: Handbook*, Canada: Elsevier Inc.