Global Journal of Management and Business Research: A Administration and Management
Volume 21 Issue 3 Version 1.0 Year 2021
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 2249-4588 & Print ISSN: 0975-5853

Role of Boards in Cyber Security Risk Profiling: The Case of Bangladeshi Commercial Banks

By Md. Bazlur Rahman, Tania Karim & Imtiaz Uddin Chowdhury
University of Chittagong

Abstract- Cybercrime becomes costlier than physical crime in developed economies. As a result, it has become the top priority in governance issues in financial institutions. As a developing nation in Bangladesh, the banking sector faces multi-dimensional challenges to adopt IT applications in banking with cybercrime. The paper examines what the banking industry faces cyber security risks and how the board members contribute to identify and mitigate the risk. Through an in-depth interview among the directors of commercial banks in Bangladesh, we identified the possible cyber risk and prepared the risk profile describing the sources, implications, severity of impact, likelihood of occurrence and ranked them. The result shows that the IT governance risk, IT investment risk, and information risk are most critical among the significant cyber security risks. The results of the study have important implications for both corporate boards and policymakers.

Keywords: cyber security, cyber risk, board governance, enterprise risk management, risk profile, top-ten risks, risk map.

GJMBR-A Classification: JEL Code: M10

Strictly as per the compliance and regulations of:

Role of Boards in Cyber Security Risk Profiling: The Case of Bangladeshi Commercial Banks

Md. Bazlur Rahman [α], Tania Karim [σ] & Imtiaz Uddin Chowdhury [ρ]

Abstract- **Cybercrime becomes costlier than physical crime in developed economies. As a result, it has become the top priority in governance issues in financial institutions. As a developing nation in Bangladesh, the banking sector faces multi-dimensional challenges to adopt IT applications in banking with cybercrime. The paper examines what the banking industry faces cyber security risks and how the board members contribute to identify and mitigate the risk. Through an in-depth interview among the directors of commercial banks in Bangladesh, we identified the possible cyber risk and prepared the risk profile describing the sources, implications, severity of impact, likelihood of occurrence and ranked them. The result shows that the IT governance risk, IT investment risk, and information risk are most critical among the significant cyber security risks. The results of the study have important implications for both corporate boards and policymakers.**

Keywords: cyber security, cyber risk, board governance, enterprise risk management, risk profile, top-ten risks, risk map.

I. Introduction

Research documented cybercrime as costlier than physical crime (Wilshusen, 2010). Malicious software alone, for instance, in recent years, caused damages multi-billion dollars. Cybercrime generated $81 million theft from the Bangladesh Bank (central bank of Bangladesh) via SWIFT. JP Morgan had data on 76 million US household account recorded stolen, and US Federal Government had $18 million personal details stolen (Danielsson, Fouché, & Macrae, 2016). Cybercrime causes financial losses and creates other risks, including reputation risk, market risk, operational risk, competency risk, and business continuation risk. The high magnitude of impact and the possibility of cybercrime leads to the use of information technology (IT) in financial institutions vulnerable on the one hand, the emergence of IT application in those institutions is robust on the other. As a result, cyber security has become the top priority list of organizations' governance issues. Identification and mitigation of cyber risk are the core functions of Enterprise Risk Management (ERM) and the board of directors must oversee these functions. Recent literature, corporate governance standards, and the legal framework of governance significantly emphasize the board's role in mitigating cyber risk among the ERM functions, especially in the financial sector. Therefore, in the financial institutions, the board members' role on the issue and their profound knowledge and IT expertise are highly required.

Information and communication technology is rapidly expanding towards every corporate sector globally, and the Bangladeshi banking sector is no exception. The use of electronic banking is growing in parts of the developing world. As the new software is introduced, existing financial transactions and services are being changed. However, still in Bangladesh, Cash is the dominant medium of exchange. During the last decade, almost all banks adopted electronic banking in thousands of branches. The banking sector faces multi-dimensional challenges to adopt and adapt

E-Banking applications fully. However, it is unclear whether the commercial banks most significantly consider the cyber risk to identify assets' vulnerability. It should also be unveiled whether the IT governance and the board governance mechanisms are adequate for cyber security. While numerous studies have investigated the means of cybercrimes and IT governance for different countries and sectors, to the best of the authors' knowledge, such studies in the Bangladeshi banking sector are absent. This study will first examine the attributes of cybercrime available in the Bangladeshi banking sector and the oversight role of boards of directors on cyber security. Our empirical analysis is based on a comprehensive survey on the impact and likelihood of cybercrimes among the board of directors of ten commercial banks operating in Bangladesh. This paper draws on cyber security risks experienced by financial institutions and identifies traditional risk management's limitations in explaining corporate boards' roles and contributions. Also, this paper focuses on the enterprise risk management (ERM) techniques on preparing the risk profile and makes three main contributions. First, the paper identifies the possible cyber risks with their sources in commercial banks in Bangladesh. Second, applying the ERM tools and techniques, the study measures the severity and likelihood and severity of cybercrimes in a time horizon. Third, it furthers our understanding of whether and how the board members contribute to identify and mitigate the cyber security risks in commercial banks. Because of the increasing pressure

Author α: Associate Professor, Department of Marketing, University of Chittagong, Chittagong, Bangladesh. e-mail: bazlur@cu.ac.bd
Author σ: Assistant Professor, Department of Marketing, University of Chittagong, Chittagong, Bangladesh. e-mail: tania_5007@yahoo.com
Author ρ: Lecturer, Department of Marketing, University of Chittagong, Chittagong, Bangladesh. e-mail: imtiazchowdhury@cu.ac.bd

to raise banking and computer technology, this study's results may have important implications for corporate boards and policymakers. The paper is divided into six sections. The second section includes the literature review, the third section outlines the methodology, the fourth section presents the results and findings of the study, the fifth section includes the discussion of the results. Finally, the last section comprises the conclusion, implication, and future research direction.

II. Literature Review

In the 1990s, when the internet emerged massively in all public and private sectors, things began to change information security management, focusing on the security related to people, processes, information, and IT. Since then, there have been many improvements taking us to where we are now with these old security management standards being changed in international standards (Humphreys, 2008). We reviewed the recent literature, reflecting on the operational risks, nature, sources, and impact of cyber risks, IT governance and risk mitigation, and the board of directors' role in risk management in the financial sector, given in the following sections.

a) *Cyber Risk and Cybercrimes*

Cyber is used as the short term for cyberspace to elucidate all-digital networks used to create, modify, store, and communicate information (GCHQ, 2012). The system includes all technical resources used in businesses, infrastructure, and services. Wilshusen (2010) identified the cyber risk as costlier than real crimes. Biener, Eling, and Wirfs (2015) refer to the term cyber risk as to the different sources of risk which affect a company's information and technology resources. They specified the cyber risk as to the business's common loss and harm arising from the technical computer system failures, thefts of data by hackers, and criminals' attacks in the system. In the USA, the National Association of Insurance Commissioners (NAIC) reported some noticeable ways of cybercrimes, including business interruption, the disclosure of sensitive information, and identity theft (Eling & Wirfs, 2016). Many studies attempted to define cyber risk from different perspectives. Some researchers focus on specific areas, such as Mukhopadhyay et al. (2013) refer cyber risk to malicious electronic events disrupting business operations.

On the other hand, many researchers define the cyber risk in a broader perspective as an information security risk (Ogut, Raghunathan, & Menon, 2011) or risk failing information systems

(Bohme & Kataria, 2006). The definition of cyber risk we employ as an expansive operational risk based on how the financial institutions categorize the cyber risk. Cebula and Young (2010) define cyber risk as an operational risk to resources in a way that affects availability, confidentiality, or integrity. In this paper, we focus on operational risks that concern IT assets.

Although a considerable amount of literature on cyber risk is found in previous studies, the empirical evidence of cyber risk in a specific industry, country or region is relatively limited. The Ponemon Institute regularly publishes reports on the number of data breaches and how they happen. The Ponemon Institute reports that in 2013, the average expense of a data breach amounting to nearly $10 million was incurred (Ponemon Institute, 2013). The report predicted the figure to be increased significantly in the following years.

Similarly, McAfee (2013) estimated a global economic impact of cybercrimes and cyber espionage for up to US$ 1 trillion each year. World Economic Forum (2012) estimate total financial losses from cybercrime in 2009 in the US alone at more than US$ 500 million. Some other studies provided more technical data for some specific countries and types of cybercrime. Danielsson, Fouché, and Macrae (2016) documented the financial loss by cybercrime in recent years in the public, private, and corporate sectors. The most significant losses and methods of cybercrime occurred recently, such as $81 million theft from the Bangladesh Bank via SWIFT,

$12 million stolen from Ecuador's Banco del Austro via SWIFT, $100 million loss caused by DRIDEX virus, data on 76 million US household account details of JP Morgan stolen, Stuxnet worm sabotaging Iran's nuclear program, and US government had 18 million personal records stolen.

b) *Nature, Sources, and Methods of Cyber Crime*

Biener et al. 2015 divided the sources of cyber risk into four broad categories: systems and technology failures, actions of people, internal processes failure, and external events. Obsolescence of hardware, failure due to capacity, compatibility of software, configuration management, security settings, coding practices, change control, system design, system specifications are the elements of cyber risk that occurred in system and technology failures. The errors, omissions, and mistakes, lack of appropriate knowledge and skills of employees, shortage of personnel to take action, intentional vandalism, theft, sabotage, and fraud are the common cyber risks in the action of people category. The internal processes failure category includes the causes of cyber risks are the failure of processes due to poor process design or inadequate execution, lack of control operating the process, and failure of supporting processes to deliver resources. The major elements of cyber risks come from external events are unfavorable weather, loss by fire, flood, earthquake, and risk arising from legal issues, changing business environment, and external parties. The ultimate impact of cybercrime is a financial loss of the organization, and the methods of crime are not always similar. Cybercrime affects the

functional departments (Accounting and Finance, Marketing, Operation or Production, Human Resources) directly or indirectly of an organization. Raghavan and Parthiban (2014) argue that cybercrime by ATM frauds, phishing, identity theft, and denial of service directly affects a firm's financing activities. Also, Raghavan and Parthiban (2014) assert that companies that fall prey to cybercriminals lose their market value because of the legitimate concerns of financial analysts, investors, and creditors and because of customers' worries about the security of their business transactions.

The cyber threats come from internal and external sources of the organization. Riem (2001) concludes that the most critical computer security threats come from employees, consultants, and contractors working in the company rather than outside hackers. In a similar study, Yapp (2001) agrees that more than 70 percent of threats to cyber security like frauds, misuses, and abuses originate mostly from the inside. The weak password policies and controls are the roots of the most internal cyber security problems.

c) *Role of Board of Directors in IT Governance and Cyber Risk Mitigation*

One of the earliest improvements in corporate governance was made in 1994 when the Toronto Stock Exchange Committee on Corporate Governance in Canada issued its report. The report included the groundbreaking guidelines for the board's role that the board of directors should explicitly assume responsibility for identifying the key risks of the corporation and ensuring the implementation of appropriate systems to mitigate those risks (Leblanc & Fraser, 2016).

Leblanc and Fraser (2016) also mentioned that, in 2010, the Securities and Exchange Commission (SEC) in the USA brought in new guidelines for the boards to involve in the oversight of the risk management functions and disclosures to the investors. Following the SEC in the USA, the UK's Financial Reporting Council, in its September 2014 publication, the UK Corporate Governance Code, stipulates that the board's responsibility is to is determine the nature and extend of the critical risks that impact on firm's strategic objectives. Also, the board should monitor the sound internal control systems.

Leblanc and Fraser (2016) emphasized the effective board governance and IT knowledge of board members. On the other hand, Kröger (2008) suggested the process and accountability of risk management relating to cyber security risks. Kröger (2008) recommended that the board should comprehensively address the cyber security issues, and finally, ensure who is responsible and who pays needs to be answered.

Shackelford (2012) argued that companies must take a proactive approach toward managing cybercrimes to improve overall cybersecurity. Similarly, Sajeva and Masera (2006) recommended that the corporate governance framework should ensure strategic guidance, active monitoring, and board accountability to the shareholders in managing cybersecurity risk.

However, many lacks on the board regarding cybersecurity governance are indeed available in the literature. Interestingly, many organizations argue that they do not need to invest enough in cybersecurity and cyber-insurance. Parent and Reich (2009) believe that this stance underscores the importance of boards to action against potential IT disasters. To make risk management decisions in a practical, fair, and rational way, Sajeva and Masera (2006) addressed that the governance strategies would have to consider a more accredited governance principle in both public and corporate levels through the participatory, efficient, and fair decision-oriented process. Furthermore, Skelcher (2005) and Renn and Walker (2008) criticized the multi-layer and complex decision making and reporting process because the present governance structures are not good enough to ensure the independence of the CIO, CRO, and other executive officers in risk reporting. Therefore, it is now generally recognized that the board has full accountability for overseeing the firm's approach to managing cybersecurity risks. However, exactly how boards do this in practice can vary. Fraser and Simkins (2010) explained some of the more popular approaches of enterprise risk oversight: first, delegating oversight of enterprise risk management to the audit committee, second, delegating oversight of risk management to the risk committee (or another existing committee such as the governance committee), third, have the full board engaged in the oversight of enterprise risk management.

III. Methodology

a) *Objectives of the study*

The primary objective of the study is to identify the top cybersecurity risks in Bangladeshi commercial banks and present their severity and likelihood through a risk profile. Also, the study demonstrates to find out whether the oversight role of the board adequate mitigating major cyber risks. The specific objectives of the study are as follows:

a. To identify the critical cyber security risks that have a significant effect on the Bangladeshi banking sector; and
b. To measure the severity and likelihood of the identified risks through the risk profiles.

b) *Study Sample, Data Collection and Analysis*

The target population for the study is the directors of banks operating in Bangladesh. We have selected ten major stock exchange listed private commercial banks operating in Bangladesh for at least 20 years and have online banking (Table -1). The

sample banks have a total of 132 directors on boards. We have collected primary data through a structured questionnaire.

Table 1: Study Sample: Commercial Banks and Assets

No.	Name of the bank	Stock Exchange Listed	Online Banking	Year of Establishment	Assets Ending 2019 in Million BD Taka	Size of Board of Directors
1.	A B Bank Limited	Yes	Yes	1982	368,076	6
2.	Bank Asia Limited	Yes	Yes	1999	355,720	16
3.	Brac Bank Limited	Yes	Yes	2001	414,855	8
4.	Dhaka Bank limited	Yes	Yes	1995	286,437	18
5.	Dutch Bangla Bank Limited	Yes	Yes	1995	380,182	6
6.	Eastern Bank Limited	Yes	Yes	1992	338,201	11
7.	Islami Bank Bangladesh Limited	Yes	Yes	1983	1,093,188	22
8.	Exim Bank Ltd.	Yes	Yes	1999	433,018	12
9.	First Security Islami Bank Ltd.	Yes	Yes	1999	437,832	14
10.	Shahjalal Islami Bank Limited	Yes	Yes	2001	268,697	19

Source: Lanka Bangla, 2020

Through a rigorous literature review, we pointed out the cybercrimes and cyber risks (Table-2) with their nature and sources. Then we asked 30 structured questions about cyber security, risk knowledge, risk profiling, and overseeing risk management functions. It is not easy to access primary data on the board of directors in financial institutions because they keep their business secret (Daily, Dalton, & Cannella, 2003). Moreover, since the directors are busy professionals, the response rate is meager (Pettigrew, 1992).

Table 2: Cyber risk and cybercrime

Type of Risk	Cybercrime
1. IT Investment Risk 2. IT Governance Risk 3. Cyber Competence Risk 4. Cyber Infrastructure Risk 5. IT Project Risk 6. Business Continuity Risk 7. Information Risk 8. Financial Risk 9. Public Perception Risk 10. IT Reputation Risk	a) Computer virus b) ATM frauds c) Identity theft d) Phishing e) Spoofing f) E- theft g) Netspionage h) Online credit card fraud i) Online denial of services j) Software piracy k) Spam l) E-fraud m) Cyber terrorism

To increase the response rate, we devoted careful attention to questionnaire design and wording of questions avoiding vague concepts and reducing items' ambiguity (Tourangeau, Rips, & Rasinski, 2000). We prepared a cover letter, emphasizing the need for research and increasing interest in the directors' topic (Minichilli, Zattoni, & Zona, 2009). We have also prepared a detailed description of the cyber risk terms and the questionnaire that allows the directors to be aware of cyber risk, cybercrimes, and risk analysis.

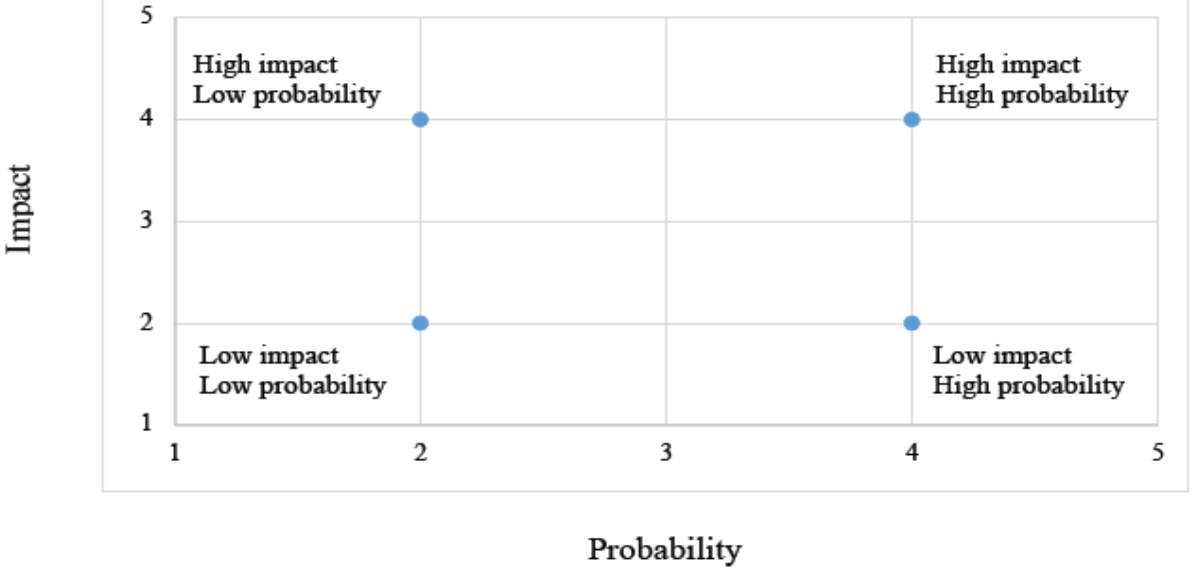
We have divided the questionnaire into three sections. In the first part of the questionnaire, we asked about the current and potential cyber risks that impact the bank's internal and external environment to assess the impact, nature, and sources of risks. In the second part, we asked to rate the impacts of identified cyber risks, and in the final part of the questionnaire, we asked to measure the likelihood of risks. We measured the impact and likelihood of risk on a five-point magnitude scale (Fraser & Simkins, 2010).

Table 3: Impact and Likelihood/Probability Scale

Rating	Impact	Likelihood Scale	Probability Scale in the Time Horizon
5 = Worst Case	Very High	5 = Very Likely	90%.
4 = Severe	High	4 = Likely	65% - 90%
3 = Major	Medium	3 = Medium	25% - 65%
2 = Moderate	Low	2 = Unlikely	5% - 25%
1 = Minor	Very Low	1 = Remote	5%

The five-point scales (Table 3) to measure risk are 1 = Minor, 2 = Moderate, 3 = Major, 4 = Severe, and 5 = Worst Case. Similarly, the impact scales are Very Low, Low, Medium, High, and Very High. The Likelihood/Probability scales are 1 = Remote, 2 = Unlikely, 3 = Medium, 4 = Likely, and 5 = Very Likely. The directors of the sample banks rated the cyber risks (Table 2). In their opinion, we assessed the impact and likelihood of the "Top 10" risks (Fraser & Simkins, 2010) with a three-year time horizon. A "Top 10" risk profile exhibits a ranked listing of the most significant risks an organization faces. It is the simplest method of identifying and ranking the risks and easy to communicate. Also, we presented the identified risks on the risk map. A risk map (Exhibit-1) is one of the most widely described ways to present critical risks facing an organization (Fraser & Simkins, 2010). It is easy to understand and exhibit, and visually appealing. The vertical axis shows the potential impact of risks, and the horizontal axis shows the estimated likelihood of risks. The map has four areas: high impact/ low likelihood, low impact/ low likelihood, high impact/ high likelihood, and low impact/ high likelihood areas. The risks falling into the area of high impact/ high likelihood are considered critical and require the extensive attention of the board and management.

Exhibit - 1: The Risk Map



IV. Results

We summarized the risk as "Top-Ten" risk (Table 4) with sources, implications/events, and possible cybercrimes in Bangladeshi commercial banks based on directors' opinions. The significant cyber risks (Top-Ten) that may happen in the banking sector in Bangladesh are IT governance risk, IT investment risk, cyber competence risk, cyber infrastructure risk, IT project risk, business continuity risk, information risk, financial risk, public perception risk, and IT reputation risk. The study results in IT governance risk as to the most significant risk in the Bangladeshi banking sector. The sources of IT governance risk are the absence of IT expert directors on the board, lack of separate board committees for IT and risk, and insufficient oversight functions regarding IT functions and cyber risk of board committees and the board of directors. The impacts of the IT governance risk on the decision-making process are delaying in the process, risk of mistake and reporting barriers to decision making, and the cost is beyond control. The respondents also agreed that cybercrimes might happen in the Bangladeshi banking

sector, including computer viruses, ATM frauds, identity theft, phishing, spoofing, E-theft, Netspionage, and online credit card fraud, online denial of services, software piracy, spam, E-fraud, and cyber- terrorism.

Table 4: Types and Sources of "Top-10" Risks

Type of Risk	Sources of Risk	Implications/ Risk Event	Cybercrime
1. IT Governance Risk	Lack of IT Expert on the Board. Lack of separate board committee for IT and Risk. I nadequate oversight function.	Delay in the decision-making process. Reporting barriers and risk of mistake in decision making. Cost is beyond control.	1. Computer virus 2. ATM frauds 3. Identity theft 4. Phishing 5. Spoofing 6. E-theft 7. Netspionage 8. Online creditcard fraud 9. Online denial of services 10. Software piracy 11. Spam 12. E-fraud 13. Cyber terrorism.
2. IT Investment Risk	Theft of Data. Hardware Damage.	Capital lost Low profit	
3. Cyber Competence Risk	Loose Customer Employee Turnover	Revenue downturn Customer dissatisfaction	
4. Cyberinfrastructure Risk	Loose Information Physical Damage	Risky Operation. Lack of insurance coverage or high insurance premium.	
5. IT Project Risk	Lack of skilled IT Expert. Lack of advanced technological i nfrastructure.	Hampered smooth operation. Long decision-making process.	
6. Business Continuity Risk	Lower Capital/Liquidity Low Business Growth	Business shutdown. Share price fall.	
7. Information Risk	Weak Password Dishonest Employee	Loosing competency. Mistrust among the customers.	
8. Financial Risk	Budget pressure/ Insufficient IT fund. High cost of IT project.	Lack of advanced technological infrastructure. Negative impact on net income.	
9. Public Perception Risk	Cyber security is not considered as top priority. Lack of prompt action against the cybercrime. Lack of updated information and community engagement.	Growing public mistrust. Reduction in using online banking and credit card. Negative reports in media	
10. IT Reputation Risk	Identity Theft. Lack of communication.	Lower customer loyalty. Additional regulatory scrutiny.	

Source: Survey opinions

Table 5: Prediction of Impact and Likelihood of Risk in Three-Year Time Horizon

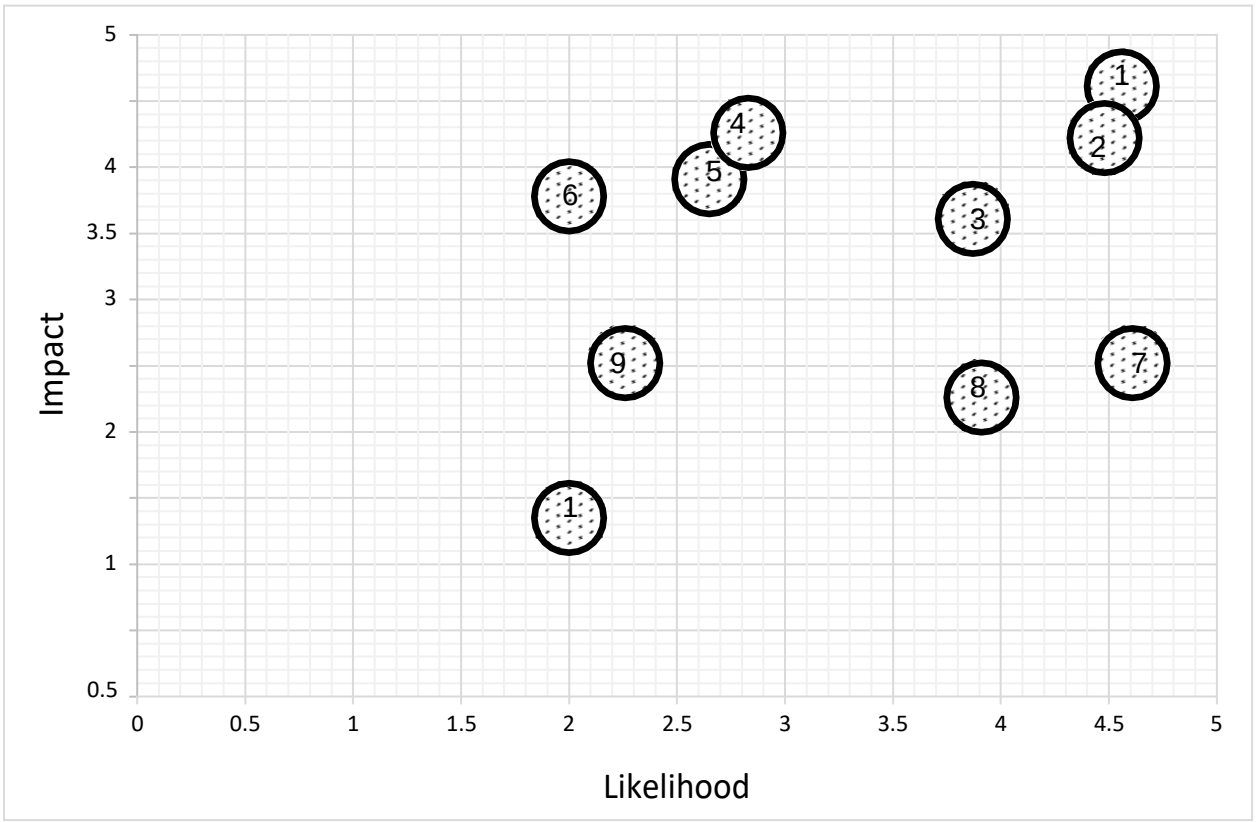
No.	Type of Risk	Impact				Likelihood			
		N	Average	St. Dev.	Magnitude	N	Average	St. Dev.	Magnitude
1	IT Governance Risk	50	4.62	0.6966	Very High	50	4.58	0.7309	Very Likely
2	IT Investment Risk	50	4.22	0.9101	High	50	4.44	0.8369	Likely
3	Information Risk	50	3.64	0.8021	High	50	3.92	1.0069	Likely
4	Cyberinfrastructure Risk	50	4.28	0.9267	High	50	2.80	0.8806	Medium
5	Cyber Competence Risk	50	3.92	0.6952	High	50	2.66	0.9172	Medium
6	IT Project Risk	50	3.78	0.6788	High	50	2.30	0.9529	Unlikely
7	Financial Risk	50	2.56	0.8609	Medium	50	4.62	0.6667	Very Likely
8	IT Reputation Risk	50	2.24	0.9161	Low	50	3.90	1.0738	Likely
9	Business Continuity Risk	50	2.48	0.8628	Medium	50	2.24	0.8466	Unlikely
10	Public Perception Risk	50	1.82	0.8003	Very Low	50	2.02	0.7421	Unlikely

Source: Authors' Figure

The respondents further evaluated the risks through a risk voting method (Fraser & Simkins, 2010), measuring the impact and likelihood of risk on a five-point scale. We summarized the voting scores of top-ten risks. IT governance risk, IT investment risk, and information risk are the most critical risks among the major cyber security risks in voting scores (Table 5). Above all, the impact of IT governance is very high and is very likely to happen. On the other hand, the cyber infrastructure risk and cyber competence risk have high impacts but medium likely to happen in the banking sector. IT reputation risk, business continuity risk, and public perception risk are identified as low significant risks.

We further presented the risk scores through the risk map in impact and likelihood magnitudes. In the risk map (Exhibit-2), IT governance and IT investment risk fall in the critical area (Red Zone), where both impact and probability are high. Information risk, cyber infrastructure risk, cyber competence risk, financial risk, and IT reputation risk fall in the alarming area (Yellow Zone) where the risk impact and probability are in medium magnitudes. On the other hand, IT project risk, business continuity risk, and public perception risk ate in the safe area of the risk map (Green Zone).

Exhibit 2: The Risk Map



Source: Table 5

V. Discussion

To investigate both existing and possible cyber risks, we gathered empirical evidence from the banking industry in Bangladesh. We combined the theories/literature about cyber security risk and IT governance and primary data to explain whether and how the risk managers and board of directors can identify and mitigate cyber security risk in the Bangladeshi banking industry. The results show that cyber security risks and their sources, impacts, and likelihood are identifiable, depending on the methods used by the organizations, and risks can be mitigated through the effective risk management process and robust oversight by the board. Hence, the board has a role in identifying and mitigating the cyber risk enhancing risk management effectiveness, and board committees' effectiveness in operational and strategic control.

Our discussion suggests that IT governance has three core targets: IT project implementation, data and information security, and hardware and systems integrity. Risk governance requires plans and implementation for each IT target. In the wake of catastrophic incidents at Target, JPMorgan Chase, Home Depot, and many other well-known established international brands worldwide, the boards of directors are now very aware of their responsibility for the safety and integrity of the data and information networks (Straight, 2015). Financial corporations are now

adopting the responsibility to monitor cyber risk management and establish three primary IT governance functions: learn, ensure, and inspect. The boards' best position is to mitigate cyber security risk and limit the damage when a cyber-attack occurs.

Similarly, the risk committee or audit committee plays a critical role in monitoring management's prevention from and response to cyber security risks and the associated regulatory framework and business developments. If all banks do not have their cyber risk committee, the audit committee may play the oversight role on cyber security risk. Implementing a successful cyber security program requires continuous and proactive engagement from the board and the risk committee. In its capacity to oversee risk management's functions and monitoring management's policies, the risk committee must play a notable strategic role in coordinating cyber security initiatives and policies.

IT investment risk arises from different types of cybercrimes, which lead to a significant loss of cyber security investment. Although banks invest a lot of money in their cyber security, the criminals break down this security and steal the data. As a result, the investment for this security becomes worthless and, consequently, the customers lose their trust and banks lose their reputation. The IT professionals' competence level falls at risk, and the new projects can face risky start for cybercrimes increasing costs.

VI. Conclusion, Implication, and Future Research Direction

In this study, using the risk profiles, we have explored whether the board of directors can identify and mitigate the cyber security risks and whether the Bangladeshi banking sector is vulnerable. The banking sector, for its vulnerability, is under the spotlight with stakeholders, including the public, regulators, media, and international agencies. Therefore, we aim to contribute to the development of cyber security in the industry by drawing attention to the board's monitoring functions. This section addresses our conclusions, policy implications, and future research directions.

This study explored the impact and likelihood of known and possible cyber risks in the Bangladeshi banking sector. We found cyber risk and their sources, events, and common cybercrimes. We employed the "Top-Ten" risk and risk map approaches to identify the most critical cyber risk that should be considered immediately. This study found that IT governance risk and IT investment risk are more critical that made the banking sector vulnerable. Also, information risk, cyber infrastructure risk, cyber competence risk, financial risk, and IT reputation risk are high in impact and likelihood magnitude. The increase of cyber risks can increase the overall risk positions, and the chance of revenues will drop, and customers can divert to competitors. Cyber incidents cause long-term intangible costs that directly impact all lines of business and, therefore, in the worst case, sharply drop the market value. Therefore, IT governance should be implemented as a process, subject to continuous monitoring, reviewing, and improvement. We find out that most of the banks do not have their separate IT committee, and very few of the board members are IT experts or IT knowledgeable. Even most of the banks do not have the position of Chief Information Officer (CIO). In contrast, Chief Risk Officer (CRO) or Chief Financial Officer (CFO) is responsible for the IT department. Consequently, the board cannot implement their IT plan appropriately and not getting specific feedback from them.

Based on the above discussion, holistic governance of cyber security risks appears to be vital in the Bangladeshi banking sector. IT governance is necessary to implement industry-wide cyber risk because of the increased importance of information and technology. We think preventive measures for IT security and coverage by cyber insurance policies can be a risk governance tool to minimize cyber risk exposures.

Moreover, the findings of the study will be helpful to planners, policymakers, regulators, including the central bank and Security Exchange Commission (SEC) of Bangladesh. The findings will be useful to stress the importance of designing and implementing a sophisticated IT governance for the financial sector to cope with the challenges and uncertainties in the changing environment arising from globalization, rapid technological changes, deregulation, and market competition.

Though our study does not concentrate on a particular governance framework, further research can be conducted on the governance framework that can effectively monitor cyber risk management to protect the firm from cybercrimes. Also, potential research can be done to determine the prevention strategies that best help individuals, businesses, and government agencies avoid cybercrime, and international best practice responses and suitable governance framework for the financial sector to mitigate cyber risk and avoid catastrophic cyber scandals.

References Références Referencias

1. Al-Hadi, A., Hasan, M. M., & Habib, A. (2016). Risk committee, firm life cycle, and market risk disclosures. Corporate Governance: An International Review, 24(2), 145-170.
2. Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. The Geneva Papers on Risk and Insurance-Issues and Practice, 40(1), 131-158.
3. Böhme, R., & Kataria, G. (2006, June). Models and Measures for Correlation in Cyber- Insurance. In WEIS (Vol. 2, p. 3).

4. Cebula, J. L., & Young, L. R. (2010). A taxonomy of operational cyber security risks. Carnegie- Mellon Univ Pittsburgh Pa Software Engineering Inst.
5. Daily, C. M., Dalton, D. R., & Cannella Jr, A. A. (2003). Corporate governance: Decades of dialogue and data. Academy of management review, 28(3), 371-382.
6. Danielsson, J., Fouche, M., & Macrae, R. (2016). Cyber risk as systemic risk. VOX CEPR Policy Portal.
7. Eling, M., & Wirfs, J. H. (2016). Cyber risk: too big to insure? Risk transfer options for a mercurial risk class (No. 59). I. VW HSG Schriftenreihe.
8. Fraser, J., & Simkins, B. (Eds.). (2010). Enterprise risk management: Today's leading research and best practices for tomorrow's executives (Vol. 3). John Wiley & Sons.
9. Greisiger, M., AllClear, I. D., Ireland, F., & Cox, P. L. L. (2013). Cyber liability & data breach insurance claims. https://netdiligence.com/wp-content/uploads/2016/05/CyberClaimsStudy-2013.pdf on, 3(01), 2017.
10. Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. information security technical report, 13(4), 247-255
11. Kröger, W. (2008). Critical infrastructures at risk: A need for a new conceptual approach and extended analytical tools. Reliability Engineering & System Safety, 93(12), 1781-1787.
12. Leblanc, R., & Fraser, J. (Eds.). (2016). The Handbook of Board Governance: A Comprehensive Guide for Public, Private, and Not-for-Profit Board Members. John Wiley & Sons.
13. Lewis, J., & Baker, S. (2013). The economic impact of cybercrime and cyber espionage. McAfee.
14. Minichilli, A., Zattoni, A., & Zona, F. (2009). Making boards effective: An empirical examination of board task performance. British Journal of Management, 20(1), 55-74.
15. Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., & Sadhukhan, S. K. (2013). Cyber- risk decision models: To insure IT or not?. Decision Support Systems, 56, 11-26.
16. Öğüt, H., Raghunathan, S., & Menon, N. (2011). Cyber security risk management: Public policy implications of correlated risk, imperfect ability to prove loss, and observability of self- protection. Risk Analysis: An International Journal, 31(3), 497-512.
17. Parent, M., & Reich, B. H. (2009). Governing information technology risk. California Management Review, 51(3), 134-152.
18. Pettigrew, A. M. (1992). On studying managerial elites. Strategic management journal, 13(S2), 163-182.
19. Ponemon Institute (2013), "Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age," http://assets.fiercemarkets.com/public/newsletter/fiercehealthit/experianponemonreport.
20. Ponemon, L. (2013). Cost of data breach study: Global analysis. Poneomon Institute sponsored by Symantec, 205-2.
21. Posthumus, S., & Von Solms, R. (2004). A framework for the governance of information security. Computers & Security, 23(8), 638-646.
22. Raghavan, A. R., & Parthiban, L. (2014). The effect of cybercrime on a Bank's finances. International Journal of Current Research and Academic Review, 2(2), 173-178.
23. Renn, O., & Walker, K. (2008). Lessons learned: A re-assessment of the IRGC framework on risk governance. In Global risk governance (pp. 331-367). Springer, Dordrecht.
24. Riem, A. 2001. Cybercrimes of the 21st Century. Computer Fraud & Security (April): 12-15.
25. Sajeva, M., & Masera, M. (2006). A strategic approach to risk governance of critical infrastructures. International journal of critical infrastructures, 2(4), 379-395.
26. Shackelford, S. J. (2012). Should your firm invest in cyber risk insurance?. Business Horizons, 55(4), 349-356.
27. Siegel, C. A., Sagalow, T. R., & Serritella, P. (2002). Cyber-risk management: technical and insurance controls for enterprise-level security. Information Systems Security, 11(4), 33-49.
28. Skelcher, C. (2005). Jurisdictional integrity, polycentrism, and the design of democratic governance. Governance, 18(1), 89-110.
29. Smith, K. T., Smith, M., & Smith, J. L. (2011). Case studies of cybercrime and its impact on marketing activity and shareholder value. Academy of Marketing Studies Journal.
30. Straight, J. (2015). The Role of the Board in Cybersecurity: 'Learn, Ensure, Inspect', Dark Reading, Retrieved on August 02, 2015, from http://www.darkreading.com/endpoint/the- role-of-the-board-in-cybersecurity-learn-ensure-inspect/a/d-id/1321222
31. Technical Note CMU/SEI-2010-TN-028, CERT Carnegie Mellon University. Tourangeau, R., Rips, L. J., & Rasinski, K. (2000). The psychology of survey response. Cambridge University Press.
32. Van Asselt, M. B., & Renn, O. (2011). Risk governance. Journal of Risk Research, 14(4), 431-449.
33. Whitman, A. F. (2015). Is ERM legally required? Yes for financial and governmental institutions, no for private enterprises. Risk Management and Insurance Review, 18(2), 161-197.
34. Wilshusen, G. C. (2010). Information Management: Challenges in Federal Agencies' Use of Web 2.0 Technologies: Testimony Before the Subcommittee on Information Policy, Census, and National

Archives, Committee on Oversight and Government Reform, House of Representatives. US Government Accountability Office.
35. World Economic Forum (2012), "Global Risks 2012 Seventh Edition," http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2012.
36. Yapp, P. (2001). Passwords: use and abuse. Computer Fraud & Security, 2001(9)