JIBC

Journal of Internet Banking and Commerce

An open access Internet journal (http://www.icommercecentral.com)

Journal of Internet Banking and Commerce, August 2019, vol. 24, no. 2

CYBER SECURITY AND DIGITALIZED FINANCIAL SYSTEM: A PARADIGM SHIFT IN GLOBAL MARKET

ALI MH

Research Associate, Taylor's Business School, Malaysia

HOSSAIN MS

Associate Professor, Department of Finance and Banking, Jahangirnagar University, Bangladesh

Tel: **+8801829590022**

Email: **sawkatfnb@juniv.edu**

UDDIN MH

Associate Professor in Finance and PhD Program Director, Taylor's University Malaysia

Abstract

This paper conducts a synthesis analysis of 'Cybersecurity and financial stability', compile the thematic areas and finally unearth the future research issues based on the researches done to date. However, the literature on this research agenda is yet at

infancy stage, although the economic aspects of cybersecurity are gaining widespread momentum and visibility in the growing body of literature. Hence the issues of cybersecurity puzzle the industry practitioners to find the possible solutions. Given this background, we make fundamental efforts to critically review the past and current studies across several thematic areas regarding cybersecurity, such as: (a) Cost issue, (b) Firm performance issue (c) Risk framework issue (d) Disclosure issue, and (e) IT development issue. The review shows that investment in cyber technology is mushrooming, nonetheless a resistant security system is yet to be achieved. Finally, with a thoughtful analysis, we compile three unaddressed research areas, such as (a) Technology and overhead cost, (b) Technology and signaling effect, and (c) Technology and risk framework. Overall, beyond the academic realm, the findings of this review could be useful to the risk analysts, bankers, and policymakers.

Keywords**: Financial Stability; Cyber Security; Operational Costs; Firm Performance; Risk Framework**

INTRODUCTION

The digitization of the global economy brings efficiency to the financial institutions and fosters financial inclusion across the globe. However, market has been facing enormous challenges due to the increasing risk of security breach which could be due to the malware, phishing mail, compromised or careless users of system, abuse of privileged access by the insiders, and targeted attacks by the external hackers, among others. These issues puzzle the industry practitioners and policy makers over the last a few decades to find out the probable solutions. Surprisingly, the contemporary researchers generally view that the cyber risk is more than an IT related technical issue as it cannot be addressed merely by technology investments. In addition, one strand of scholars claims that the impact of cyber technology spurring the economic growth, whilst the

other strand of scholars strongly believe that the positive outcome of technology has already been reaped up. The reason for having the later proposition could be due to the negative externalities arising from the wide innovation, acute competition in banking sector leading lower profit margin, the cost of maintaining adequate cyber security in banks, the loss from cyber-crime seem to raise the operational overhead, among others. All of these consequences can lead to higher cost to income, and thereby adversely affect the firm performance [1-31].

Based on the recent occurrences provided by the institutions' website, newspapers, policy report, we find that the cybercrimes are taking place more frequently in the financial sector, particularly in the banking industry. For instance, Russian hacker steals about 30,000 customer credit card credentials from an internet music store named CD universe. The hacker posts thousands of numbers on his website after the company refuses to pay $100,000 as ransom demand. Similarly, a hacker copies the information of 15700 credit and debit cards from the western union website in 2001 [32]. The theft of third-party information is likely to spur legal liability and threats of lawsuits on the breached party. Surprisingly, this sort of information immediately injects negative perception in the market which reflects the fall of share prices. This proposition is supported by the earlier study of Garg [32] who claims that there is a positive correlation between the number of credit cards hacking and the share price decline.

Moreover, the recent phenomena[1] over the last few decades show a huge loss in the economy, and thus leave the financial sector consisting of money market and capital market unstable. For instance, Bangladesh central bank loses US$81 million to hackers in 2016 [33], Vietnam's Tien Phong Bank suffers USD one million losses due to cyber-crime incidence in 2015 [19], Banco Del Austro in Ecuador faces USD 12 million financial loss in 2015 [30] and Carbanak incurs a total of one billion USD loss due to several cyber-attacks in 2014 [33-44]. These examples show the tip of the iceberg of the cybersecurity risks in the global financial industry that not only causing the substantial financial losses but also eroding the confidence in the financial system.

[1] Please see the appendix 1(b) for details of the recent cyber incidents across the globe based on the newspaper report.

Therefore, the institutions around the world have been investing heavily to build up a secure cyber infrastructure. For instance, the Canadian Bankers Association announces to invest $70 billion on technology upgrading and Bank of England plans to spend £2 billion for stronger cybersecurity. In this regard, statistics show that direct cyber security spending of the firms including financial institutions accounts for about 0.1% of the global GDP in 2015 [39]. Hence having considered the analysis, we find that cyber security is a burning issue which should be addressed with much importance.

Therefore, there have been a dilemma surrounding the inherent financial effect of cyber-crime. On the one hand, financial institutions incur direct cost for cyber incidents, these include forensic investigation cost, customer notification cost, the cost for post-breach customer security and credit protection, and pre-measures to strengthen cybersecurity system, legal assistance, cost for staff training and development with upgrade IT system, third party cloud and security providing cost. Hence cyber-crime includes additional operational expenses and decreases the profitability of the financial institutions. On the other hand, indirect costs are in long term nature and challenging to quantify ex-ante. Those indirect cost include the negative effect of cyber-crime on stock prices and volatility, negative image on brand name, issue of reputational risk, loss of depositors in the financial institutions, and liquidity crisis in the event of cyber breach incident, among others. Thus, the stability of financial institutions, particularly the banks is now under the threat of severe cyber security risk [45-47].

The consequence of cyber security is remarkably persistent in the financial market. For instance [48], discuss on how the cybercrimes impose a financial burden on the banking institutions and the difficulty of estimating losses as a cyber incidence emits effects in different ways. We also observe that cyber crimes are now exposed to be a big operational risk as well as reputational risk for the financial institutions. The impact of these risks is very complex and unmeasurable. In this respect a study [45] show that cybersecurity risk leads to higher operational costs, lower revenue, lower equity value, customer loss, brand loss, and reputation damage. In addition, Fitch rating agency explains that cyber risk can adversely affect financial results of the institutions [31,48]. Furthermore, the International Organization of Securities Commission's Committee

(IOSCC) on Payments and Market Infrastructures and G7 cyber risk expert group mention that cyber risk is very crucial for financial institutions as well as in the capital market. Thus, the failure of cyber security may have a notable signaling effect in the market that may adversely affect the investors trading behavior.

Research Objective

This paper aims to conduct a systematic review on the existing and germane quantitative as well as qualitative studies on the issue of cyber security from the context of finance and accounting and then explore the future research gaps. We find that cyber security has been an ongoing issue and also the number of hacking incident is on the rise until today. Despite the incremental rise of cyber incident, the prior research on cyber security is still limited and mainly on discussion-based as well as qualitative type. However, in this paper, we argue that cyber security cost has an effect on banks profitability, market performance and the financial stability. In summary, the synthesis summarizes a bundle of key thematic areas, such as- in section 2.1, we illustrate that the technology cost consisting of investment in computer development, expenditure in software installment and upgrade, cost to train up staff, cost to cloud and security protection provider, affects the profitability in the banks. It is still a debatable issue if technology cost follows a linear or non-linear relationship to bring benefits to the banks. Then in section 2.2, we illustrate how the cyber security breach tagged as bad news affects security prices and price volatility in the market, because there is a growing demand that security breach incident pushes down the security price in the capital market. We strive to capture cyber security news either positive or negative or even neutral. Finally, in section 2.3 we mention that despite the cyber security being a momentum issue in the financial sector, there is still a lack of cyber-security risk management framework. Though there are few countries like USA, UK, Singapore and Hong Kong use cyber security risk management framework, however several other countries still feel lack of standardization in the cyber-security risk management.

Research Question

The study addresses several motivating research questions, such as: (a) Does CyberTech investment affect banks profitability? (b) Do cybersecurity compliance disclosures affect the banks' probability of being hacked? (c) Do banks focus more on the cybersecurity management and risk disclosure in comparison to increasing investment in CyberTech to enhance financial stability? Let us now review the existing literature of cybersecurity to develop the research issues and eventually, the final section wraps up with the summary of cybersecurity literature review.

Literature Review

The emergence of technology in the 21st century has revolutionized every walk of human life. However, interestingly banking in this century flourishes with a wider set of opportunities and challenges as a result of technology. Internet in the banking industry is good for economy as it reduces the associated cost in the transaction. From macro-economic perspective, e-commerce business due to banking technology has been easier for customers since they can transact online anywhere anytime and thus it has increased the consumption trend. Technology in the banking not only influences the economy of scale by competitive pressure but also affects the economies of delivery by a wide range of alternative delivery i.e. ATM, Net banking, credit card online, mobile banking, bill payment, shopping, and ticket booking, among others [20]. Hence information technology reduces the operating expenditure, as well as improve customer services by assisting the banks to introduce new products and services [49-67].

Moreover, technology has a substantial effect on banking sector both internally and externally [18,22,36,42,50,52,58]. In addition, another strand of scholars claim that technology in the banking industry has reduced the overhead cost [23-25,35,38,55,68]. In addition [35] opine that technology adoption is negatively associated with bank risk, technology make the customers data available and transparent for loan-sanction

decision and thus likely to reduce non-performing loan, yet a big question still remains unaddressed about the hacking risk due to inappropriate cyber security measures. However, remaining in positive, technology improves the production function of banks and industry wide scale economies [21,40].

Empirically, opposite to that [47] find that there is a negative relationship between bank holding company size and non-interest expense. Profitability in technology equipped banks is lower than those without technology and expenses are higher in internet banking [4,62]. Since the cost associated with new apps installation, system upgradation, security cost against cyber peril, computer set up, training employees as well as third party supervision cost, and that is how banks seem to be incurring substantial overhead expenses. Surprisingly enough, technology may no longer a support function in financial sector according to monetary authority of Singapore, perhaps because of the technology maintenance cost is exponentially increasing and more importantly due to the increase of cyber peril day by day. Further, cybersecurity area expert authority Fitch rating explains that cyber risk can adversely affect credit ratings, and thereby causes detrimental operational and financial consequences.

Technology and Overhead Cost

We notice that 21st century's banking system has seen the exponential revolution happened by the information technology. Due to the rapid expansion of technology, as of now, banks come with new products and services for the customer. At present, the financial market becomes more transparent and efficient which makes customer to choose the best alternative products and services. Thus banking sector has become much more competitive than ever. We find that different types of costs are associated with new apps installation, system upgradation, security cost against cyber peril, computer set up, training employees as well as third party supervision cost, and that is how banks seem to be incurring substantial overhead expenses. The technology costs fall under the ratio of overhead to total asset. Further, it is important to understand the separation of ratio of technology overhead to total asset and the higher the ratio means

the lower the profitability. Hence, technology cost could possibly reduce the profitability of banks.

Internet expense in the banks is a fixed overhead which leaves the profitability more volatile or higher operational leverage. Technology based banking attributes lead to the rise of bank's overall risk profile as risk associated with financial services [57]. The increase of cyber security breach and hacking incidents across the banks as well as the overall maintenance of the whole network system leads to the increase of operational risk. In this respect, Antonescu et al. [8] discusses about the key motives behind cyber security investment, which are process improvement, risk reduction, regulatory compliance and cost reduction. Böhme [13] demonstrates the relationship between security investment and security Metrix by using cost to income ratio in terms of production function. Most of his discussion is to balance between cyber security investment cost and the benefit arising from this investment. In addition, Kox [46] finds that internet has become a safer place in compare to the number of cyber incidents but he leaves serious concerns to be taken care of in future. The reason is that customers lose their personal data and money after cyber-attack which paves the way for customers to loss trust in the banks and thus reputational risk arises.

Unfortunately, during this ever since-peak time of Fin-tech, Crowdfunding, Cryptocurrency and Sandbox, we are in a big dilemma on whether bank's expenditure on technology is good or bad to its profitability? Even though, there have been lots of researches in this area [18,22,36,42,50,52] supported that technology is good for banks whilst [4,47,62] found bad for bank but no research so far is considering directly the cost into the technology which covers apps installation, system upgradation, security cost against cyber peril, computer set up, training employees as well as third party supervision in the bank's income statement. Most of the previous research done considering the effect before and after technology adoption and the rest takes account the ATM machine, Online Branches, Debit and Credit Card or even Online transaction and some other counting website system. Reasons could be the lack of disclosure issue, scarcity of data, and then cyber security was not a hot issue to consider with much importance in the past. Also, the country-level regulators have been issuing policy

guidelines for managing the operational risk arising from cyber technology use[2]. Hence, the cybersecurity risks that are rapidly growing with the digital transformation of operational paradigm in the financial sector as well as in the broader society has become a critical concern to maintain the resiliency of financial system, but the body of academic literature in this field is yet at infancy stage.

So, the existing issue and studies pave the way for future research on whether technology cost (technology cost to total asset ratio) affects the profitability of banks. Hence the key question is whether the marginal benefit from an additional cyber investment is more than the marginal cost of its operations. This is a pertinent question because the use of technology improves operational efficiency but it also contributes to direct overhead costs [17,47] in addition to the risk of cyber breach. Moreover, it is enormously difficult to assess the non-tangible and indirect costs associated with the security system breaks [9,27]. The non-tangible cost includes the loss of reputations and customer confidence while indirect costs are the expenses for system recovery, litigations, and compensation [41,45]. Therefore, it is difficult to determine the level of optimal investment in IT security system but this should be based on the analysis of costs and benefits from IT investment. As building and maintenance of the IT infrastructure require a substantial amount of capital investments and fixed operational costs, the cybersecurity and information technology become important topics in the corporate boardroom discussions [16]. This is because the rise of fixed overhead costs for IT infrastructure maintenance could make the corporate earnings of financial institutions more unstable - set aside the intangible and indirect costs.

Technology and Signaling Effect

The equity price moves up and down with time due to the demand and supply for the respective company's share. There are several factors affecting company demand and

[2] We find that as of now Basel committee identifies, describes and compares the range of observed bank, regulatory, and supervisory cyber-resilience practices across jurisdictions (Basel Committee, 2018). Also, Uddin & Ali (2019) provides a summary of cyber risk management guidlines by different the international agencies and country-level reguators.

supply of share such as company performance, economic performance, industry performance, investor's sentiment, and any news of scandal, unexpected incident as well as negative shock of company. News could be perceived as positive and negative, however the positive news about good performance, good governance, and better risk management pushes investor to buy the stock. To the contrary, negative news like, bad performance, bad governance, bad risk management and scandal influence investors to sell the share and thus fall of share prices. This is simply because the market is converting future expectation into prices.

Signaling theory is crucial to describe the behavior of stakeholders immediately after they have new information. The responsiveness of the stakeholders is explained by this theory. The whole idea is how the investors interpret the signal either positively, negatively, or even neutrally. The usage of signaling theory has gained momentum as the market has been exponentially digitalized where information is reaching out within shorter time. However, pertinently, the cyber security breach can be interpreted as an effective signal and can therefor strongly affect the prices of share. Tetlock et. al [64] says that news carries qualitative information influencing the expectation of investors about firms' future performance. Investors are rational and an efficient market reflects all known information available in the market.

Behavioral finance describes how the psychological factors affect the financial market evolution. However, the efficient market hypothesis explains the market where any information is available to all. In another word, the price of stock should reflect the knowledge, information and expectation of all investors. So, stock price reflects all relevant information irrespective of positive and negative. Informational efficiency is mirrored by the instances where stock prices fully reflect all market available information regarding the company. In another word, the informational efficiency captures the speed and accuracy of prices which reflect the new information. In this respect, Malkie says that a capital market to be efficient if it reflects all information available. But, the argument is whether the investors behave rationally or irrationally after the negative news of cyber breach, since the expert claim is there is a fall in the share price following

cyber-crime news in the media. It is found that individual equity reacts more to the negative earning news than good earning news during the good times [7].

Therefore, the negative news on cyber security breach affects the equity price in the market. Because the volume of share traded in the stock market and the activity is linked to pessimism and its interaction with media news. The market in the respective area is insignificant when there is no news available in the market, and Engelberg and Parsons show that local news from local perspective influence the market activity. Hirshleifer et al. illustrates that investors are the net traders following both good and bad earning news. However, Lee conjectures that news can attract investors' attention or can routinely contact their investors around the time of earning declaration. Further research by a group of scholars recently documents that the equity market is affected by the information published in different public media, which change the individual stock prices as well as the overall stock market [14,54,63,66]. However, Veronesi [66] further explains that stock market is likely to responds higly to bad news in good times. That could be because of psychological factors of behavior as Bondt et al. finds in his experimental study that most of the people overreact to unexpected and surreptitious news events. Thus, we can conjecture that negative news about the company cause investor to overreact in their trading behavior.

Cyber-crime affects depositor's confidence as well as stock holder's confidence as a fact that they can no longer trust into their security system broadly operating system and they are scared of further revealing their personal data and loss of their money. Experts say that cyber-crime bring the instability in the stock prices of cyber-breached firm. The destruction of critical system and theft of data and money by the cyber-criminals make a financial and operating loss for the firm. Watkins [67] discusses the increase of malicious activities hints that organizations can no longer avoid the unavoidable cyber threat. The calculation of cyber-crime cost is not easy as its affect comes in multiple channel such as, higher operating cost, loss of depositors in the bank, stock prices volatility and also good will issue. Lewis and Baker [48] discuss the economic impact of cyber-crime and conclude that cost of cyber-crime is difficult because it has effect from many fronts. Cyber-crime has been exposed a big operational risk as well as

reputational risk. The impacts of both risk is much more complex than a straight forward. In this respect, Kopp et al. [45] shows that cyber security cost includes the higher operational cost, lower revenue, low in equity value, customer loss, brand loss, and reputational depreciation for long term, among others.

However, quantitative economic analysis in the arena of cyber security has been hindered due to the lack of data availability. Few researches done in cyber security area, for instance, Saini, Rao and Panda [60] demonstrate conceptually cyber risk, cyber-crime' effect on economic disruption i.e. impact on operational cost, impact on market value as well as customer trust. Hereby to support the claim, the empirical study is missing. Antonescu and Birău [8] investigates the financial and non-financial effect of cyber-crime in the emerging countries, however that is also lacking the quantitative support. Hemphill [37] explains about the financial data breaches in the US retail economy and restoring confidence in information technology security standard and also what technology improvement can really bring more security protection of customer data and thus ensuring the protected system. Bhasinm [10], and Algarni [5] find the reasons of frauds in the banks and to develop the approaches to make stronger security against data breaches. Peeters [56] discusses the different procedures for disclosure that could be most valuable for cyber resilience. Hall et al. [34] conduct a survey and finds that internet is facing challenges in keeping its interconnection system resilient. Tendulkar [65] demonstrates cyber-crime security market and systematic risk and also says that a large scale cyber-attack may damage the market efficiency and integrity. Morever, the direct cost to Europe of electronic crime, including both losses and protective measures, is measured in billions of euros; and growing public concerns about information security hinder the development of both markets and public services, causing even greater indirect costs [6].

Prior literature on finance explores the linkage between the tone of news in the form of sentiment to its stock price returns, volatility, trading turnover as well as company performance [49,64]. These researchers find that negative words in the public news media affect the company’s stock prices as well as performance. Similarly, Loughran and MacDonald [49] find the significant effect between the fraud news and return

volatility, trading volume. As regulators, economists, bankers, risk analysts and academicians claim that there is a reduction or higher volatility in the stock prices following security breach incident in the news media, and no empirical study to support that claim; and therefore it remained unanswered up to date. Overall, the cybersecurity risk being a time-variant innovative hazard is very different from other types of risk exposures for the financial institutions - such as credit risk, liquidity risk, interest rate risk, and market risk. The plausible reason is that the magnitude of the cyber risk exposure is yet unknown but it certainly has a colossal effect on the earnings and growth of the financial institutions as we have reviewed above. Thus, cybersecurity concern increases the overall riskiness of the financial institutions, and the stakeholders such as depositors and equity holders may require an additional risk premium from the institutions that are weak in cyber risk management.

Technology and Risk Framework

The recent technological development leads to the rise of the number of cyber incident happening across the world, surprisingly cyber incidents are occurring more in the financial sector. We notice that banking sector has been of galloping target to the hackers. Few of the hacking events occurred in the last few years are, Tesco bank incurs two million pounds due to cyber-attack, whilst, Bank of Russia counts loss around $31 million in 2016. In addition, we find that Bangladesh Bank faces US$81 million loss hacked by hackers in 2016 [1], Vietnam's Tien Phong Bank counts one million USD loss by cyber-crime in 2015, Banco del Austro in Ecuador faces 12 million USD loss in 2015; and Carbanak incurs a total of one billion USD loss by the cyber-attack in 2014. Further, HSBC is attacked by distributed denial of service. Consequently, this recent phenomenon is more oriented to provide solution to this uprising hacking threat.

The effective cyber risk management is important at the micro level to support financial stability at the banks and financial institutions. It is also critically important at the macro level for the financial integrations, financial inclusions, and financial deregulations [7,42]. Since the risk of cybersecurity breach has been evolving and growing at a faster speed

in tandem with the increasing IT penetration in banking operations, the cyber risk management primarily aimed at IT-based solutions focusing on the fixing up system loopholes [2,53]. However, the industry experts and practitioners suggest non-IT based approaches alongside technical solutions to manage cyber risk more effectively. As banks' strategic focus is shifting towards developing either in-house technology infrastructure or making a partnership with fintech firms[3], the business operational risk is also escalating due to increased technology interdependencies between the banks, and even between the banks and fintech firms.

Therefore, it is a must to have proper cyber security risk management framework in place as like as other risks, such as market risk, liquidity risk and credit risk. The recent prepared cyber risk management framework for financial institutions by USA, UK, Singapore, and Hong Kong are under criticism by the scholars while the standardized, harmonized and time-varying cyber risk framework are of crucial importance. The first managerial approach is to frame policies to tackle the risks associated with the breach of the cybersecurity system by the external and internal parties [26,59,61]. This includes, among others, the detection and mitigation of cyber threats, budgetary allocations for covering the losses from cyber incidences, and adoption of cyber insurance. The restructuring of the organization includes setting up of an independent cybersecurity task force combining the personnel with technical, operational, and legal backgrounds [34]. This task force, being a multi-skill team, can detect the system loopholes, potential threats, financial losses, and legal consequences and mitigation measures to protect the interests of the banks and their customers. The capacity building measures include acquiring and upgrading of the relevant hardware and software, deploying a well-skilled technical team, arranging mandatory cybersecurity training for the employees, offering regular workshops on the importance of ethical behaviors, enhancing the security alertness among the customers and end-users of the banking services [51]. Banks need to effectively collaborate with the external vendors or

[3] As the traditional banks face challenges to innovate due to the lack of management focus and internal capabilities, cooperation with fintech firms is a prominent option to foster banking innovations and maintain the market share during the period of technological revolution (Drasch, Schweizer, & Urbach, 2018).

agencies offering the hardware and software because the cybersecurity risk stems from the technical sources and the solutions also primarily come from these external parties. Finally, the top management ensures compliance of the internal policies and regulatory requirements regarding the cybersecurity risk management. However, to come up with that cyber risk model would be a great contribution to every jurisdiction as cyber security risk is homogeneous type which does not varies across cross-border. So, with the rise of cyber risk[4], it becomes an immediate necessity for the financial institutions globally building up a more resilient but efficient cyber technological infrastructure

Therefore, based on the review of policy documents of different international agencies and countries, we summarize the following common elements of cybersecurity management practices globally: (*A) Risk awareness:* Create awareness of the consequences of cybersecurity risk among all stakeholders; (*B) Reporting incidences:* Report cybercrime incidents immediately to all stakeholders in a transparent manner; (*C) Security department:* Establish a unit responsible for security of information system and cyber risk related matters; (*D) Appraisal and response:* Develop a broad-based risk assessment and response system that identifies the security threats and vulnerabilities from the technological and non-technological sources such as human factors, security policies, and third-party vendors; (*E) Preventing threats:* Detect and prevent cyber threats as the part of an integrated risk management system that integrate both technical and non-technical measures; (*F) Training management:* Arrange education and training to build human capital capable of managing cybersecurity issues effectively; (*G) Collaboration and cooperation* Ensure collaboration and cooperation with relevant agencies at the national and international levels to enhance a more resilient IT infrastructure; (*H) Ethical standards:* Promote ethical standard among the stakeholders, particularly those responsible for the management of security system management.

[4] We find that Financial Times clarifies cyber-attacks on financial services sector in the UK rise fivefold in 2018 (Murgia & Megaw, 2019). An article at Harvard Business Review suggests cyber-attack could cause the next financial crisis because cyber-attack might disrupt financial services capabilities, especially payments systems, around the world. Such an attack could erode market confidence in the global financial system drastically, which in turn could negatively impact global economy.

KEY FINDINGS

We find that cyber security risk is a new fundamental research issue of the modern economy that needs more in-depth analysis to know about the dynamics of emerging problems affecting global financial stability and identify sustainable solutions. The key findings of the study are highlighted below:

Findings	**Potential solution**
The study finds that the between Cybertech cost and bank performance is still not done yet.	The potential gap could be filled with technology cost (mostly for better safeguard from cyberattack) by considering relevant cost from the bank financial statement.
The study explores the missing studies on the impact of cyberattack immediately on the stock market price of victim bank.	There could be a study on this area considering the textual massage in the public knowledge.
The study finds no academic literature considering the cybersecurity risk into the risk management and how it needs to be managed despite it has been a boardroom issue in the existing literature.	There can be a study dealing with cybersecurity risk adoption, adjustment and management in the risk management framework.

DISCUSSION

In this study, we make efforts to take the stock of prior studies on the cyber security issues and their consequences on the financial stability. In summary, the systematic review of cyber security literatures unearthed the future research issues regarding cyber security risks and evaluates them in the context of finance and banking. We find that the literature studying cyber security effects on the financial stability is not yet adequately

developed but we know to some extent the dynamics of the links between the cyber risks and financial instability. In a nutshell, this review paper summarizes five thematic areas in which prior academic researchers and industry practitioners have contributed and proposes three key areas in which more in-depth study is necessary. Therefore, this review paper is a groundbreaking for the researchers to take forward the future researches on cyber security and financial stability – an emerging research field in the technology-driven finance industry.

This is the first paper that contributes to our understanding of why and how the infusion of digital technology could destabilize the global financial industry and develop an integrated new risk management framework. Overall, beyond the academic realm, the findings of this review could be useful to the risk analysts, bankers, and policymakers.

CONCLUSION

Cyber threats are appearing as the systemic phenomena since our society gradually moving towards the digital environment in which the institutions and their stakeholders communicate and undertake transactions remotely through online system. In the online based communications, unauthorized access to the system may trigger an economic shock leading to the failure of a financial institution due to the systemic effects across the networks [43]. This systemic effect can be more catastrophic for the financial institutions in some instances [15]. For example, if a bank is unable to settle its net debts (due to intruders' attack) within the interbank transaction settlement system, the other parties within the network might also be unable to settle their commitments – leading to financial system failure [29,65]. Therefore, the policy makers and regulators recognize that a cyber intrusion not only affects a single institution but also disturbs different elements of the entire financial network and other service providers [28]. This means the growing tendency of breaching cyber security system by unauthorized intruders may lead to widespread impacts on the economy because of the payment system breakdowns, confidential data leakages, and wider infrastructure failures across different service providers and organizations [12]. Overall, we find the cybersecurity risk

and its potential consequence are buzzing issues that are hardly examined from an academic point of view[5]. Hence, the international body governing the global financial market stability suggests enhancing cyber resilience in the financial institutions across the world [11].

Therefore, cyber invasion appears to be systemic phenomenon in the financial system that can be mitigated through improving cyber resilience within the financial institutions.

References

1. Ackerman K (2016) Is Cyber Risk Systemic? New York: American International Group.

2. Akhawe D, Barth A, Lam PE, Mitchell J, Song D (2015) Towards a Formal Foundation of Web Security. 2010 23rd IEEE Computer Security Foundations Symposium pp: 290-304.

3. Akhawe D, Barth A, Lam PE, Mitchell J, Song D (2010) Equifax breaks down just how bad last year's data breach was. NBC News.

4. Alam U, Ahmad N, Schreyer P (2007) Measuring GDP in a Digitalised Economy. OECD Statistics.

5. Algarni A (2016) Financial Sector's Cybersecurity: Regulations and Supervision. Washington, United States of America: World Bank Group.

6. Anderson Y, Antonescua M, Birău R (2009) Financial and non-financial implications of cybercrimes in emerging countries. Procedia Economics and Finance pp: 618-621.

7. Arner DW, Barberis J, Buckley RP (2016) FinTech, RegTech, and the Reconceptualization of Financial Regulation. Nw J Int'l L & Bus pp: 51.

8. Antonescu M, Birău J (2015) Bank Capital for Operational Risk: A Tale of Fragility and Instability. Journal of Risk Management in Financial Institutions 8: 227-243.

[5] A summary of the findings of notable published papers on Cyber Security Issues is presented in the Appendix.

9. B¨ohme R (2010) Security Metrics and Security Investment Models. Advances in Information and Computer Security pp: 10-24

10. Bhasinm I (2015) Cybercrime: The Cost of Investments into Protection. Journal of Criminal Justice and Security 105-116.

11. BIS (2016) Bank for International Settlements.

12. Boer M, Vazquez J (2017) Cyber Security & Financial Stability: How cyber-attacks could materially impact the global financial system. Washington: The Institute of International Finance.

13. Böhme A (2010) Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience. Journal of Contingencies and Crisis Management 15: 50-59.

14. Caporale L, Burden K, Palmer C (2016) Internet crime: Cyber Crime - A new breed of criminal? Computer Law & Security Review 19: 222-27.

15. Carey M, Stulz RM (2008) The Risks of Financial Institutions. Journal of Contingencies and Crisis Management 16: 65-66.

16. Carl Colwill (2009) Human factors in information security: The insider threat – Who can you trust these days? Information Security Technical Report 14:186-196.

17. Cavusoglu H, Raghunathan S, Yue WT (2008). Decision-Theoretic and Game-Theoretic Approaches to IT Security Investment. Journal of Management Information Systems 25: 281-304.

18. Ciciretti M, Smith RG, McCusker R (2009) Future directions in technology-enabled crime: 2007–09. Canberra: Australian Institute of Criminology.

19. CNBC (2016) Vietnam's Tien Phong Bank says it was second bank hit by SWIFT cyberattack. CNBC.

20. Dangolani S (2011) Transforming cybersecurity in the Financial Services Industry. Deloitte.

21. Daniel K, Crisanto JC, Prenio J (1973) Regulatory approaches to enhance banks' cyber-security frameworks, Financial Stability Institute.

22. De-Young A (2005) The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution. The World Bank.

23. De-Young DW, Dybvig PH (2007) Bank Runs, Deposit Insurance, and Liquidity. Journal of Political Economy 91: 401-419.
24. Dow Z (2007) Blockchain: a secure, decentralized, trusted cyber infrastructure solution for future energy systems. Journal of Modern Power Systems and Clean Energy pp: 1-10.
25. Downes K, Mui G (1998) Capturing flexibility of information technology infrastructure: A study of resource characteristics and their measure. Journal of management information systems 12: 37-57.
26. Dutta A, McCrohan K (2002) Management's Role in Information Security in a Cyber Economy. California Management Review 45.
27. Eling M, Lehmann M (2018) The Impact of Digitalization on the Insurance Value Chain and the Insurability of Risks. The Geneva Papers on Risk and Insurance-Issues and Practice 43: 359-396.
28. EU (2018) The Directive on security of network and information systems (NIS Directive).
29. Fed (2017) Federal Reserve Policy on Payment System Risk. Washington, USA: Federal Reserve System.
30. Finch G (2016) Ecuador Bank Says It Lost $12 Million in Swift 2015 Cyber Hack. Bloomberg.
31. Fitch (2017) Cybersecurity an Increasing Focus for Financial Institutions.
32. Garg A, Curtis J, Halper H (2003) The financial impact of IT security breaches: what do investors think? Information Systems Security 12: 22-33.
33. Gopalakrishnan R, Mogato M (M2016) Bangladesh Bank official's computer was hacked to carry out $81 million heist: diplomat. Thomson Reuters.
34. Hall U, Granåsen M, Andersson D (2013) Measuring team effectiveness in cyber-defense exercises: a cross-disciplinary case study. Cognition, Technology & Work 18: 121-143.
35. Hasan G, Zazzara A (2009) Outsourcing the is function: Is It Necessary for Your Organization? Information Systems Management 9: 44-47.

36. Hagel LA, Loeb MP (1997) Information Systems and Developing Countries: Failure, Success, and Local Improvisations. The Information Society 18: 101-112.

37. Hemphill K (2016) Exploring stolen data markets online: products and market forces. Criminal Justice Studies 23: 33-50.

38. Hernando L, Nieto T (2007) Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support System 47: 154-165.

39. Hughes BB, Bohl D, Irfan M, Margolese-Malin E, Solórzano J (2017) Cyber Benefits and Risks: Quantitatively Understanding and Forecasting the Balance. Extended Project Report from the Frederick S. Pardee Center for International Futures.

40. Hunter G, Timme R (1991) Enhancing Bank Transparency: A Re-assessment. Review of Finance 6: 429-445.

41: Ismail N (2018) https://www.information-age.com/data-breaches-financial-impact-123470254/.

42. Jayawardhena C, Foley P (2000) Changes in the banking sector – the case of Internet banking in the UK. Internet Research 10: 19-31.

43: Johnson KN (2015) Managing Cyber Risks. Georgia Law Review 50.

44. Kaspersky (2015) The greatest heist of the century: hackers stole $1 bln.

45. Kopp E, Kaffenberger L, Wilson C (2017) Cyber Risk, Market Failures, and Financial Stability, Working Paper. International Monetary Fund(WP/17/185).

46. Kox, HL (2013) Cybersecurity in the perspective of Internet traffic growth. Working paper. CPB Netherlands Bureau for Economic Policy Analysis.

47. Kovner O, Kunreuther H, Heal G (2014) Interdependent security. Journal of Rsk and Uncertainty 26: 231-249.

48. Lewis J, Baker S (2013) The Economic Impact of Cybercrime and Cyber Espionage. McAfee.

49. Loughran K, MacDonald U (2011) Insuring against cyber-attacks. Computer Fraud & Security pp: 18-20.

50. Mandeville T (1998) Critical Infrastructure (1st ed.). Boca Raton: Taylor and Francis Group.

51. Mayahi A, Humaid I (2016) Development of a Comprehensive Information Security System for UAE e-Government. PhD thesis, Prifysgol Bangor University.
52. Mishkin S, Strahan H (1999) Systemic operational risk: does it exist and, if so, how do we regulate it? The Journal of Operational Risk 8: 59-99.
53. Morton M, Werner J, Kintis P, Snow K, Antonakakis M, et al. (2018) Security Risks in Asynchronous Web Servers: When Performance Optimizations Amplify the Impact of Data-Oriented Attacks. IEEE European Symposium on Security and Privacy, pp: 167-182.
54. Neuhierl K, Page J, Kaur M, Waters E (2013) Directors' liability survey: Cyber attacks and data loss-a growing concern. Journal of Data Protection & Privacy1: 73-182.
55. Petersen D, Rajan P (2002) Recovery Oriented Computing (ROC): Motivation, Definition, Techniques, and Case Studies. UC Berkeley Computer Science.
56. Peeters G (2017) Strengthening the digital Achilles heel of the European Union: Make use of ethical hackers to find vulnerabilities in information systems? Master thesis.
57. Pennathur C (2001) Modelingandpredictingextremecyberattackratesvia markedpointprocesses. Journal of Applied Statistics 44: 2534-2563.
58. Prescott J, Van S (1997) Regulatory approaches to enhance banks' cyber-security frameworks. Financial Stability.
59. Ralston P, Graham J, Hieb J (2007) Cyber security risk assessment for SCADA and DCS networks. ISA Transactions 46: 583-594.
60. Saini H, Rao F, Panda L (2012) The Market Reaction to the Disclosure of Supervisory Actions: Implications for Bank Transparency. Journal of Financial Intermediation 9: 298-319.
61: Soomro ZA, Shah MH, Ahmed J (2016) Information security management needs more holistic approach: A literature review. International Journal of Information Management 36: 215-225.

62. Sullivan D (2000) Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors. Decision Support Systems 49-62.
63. Tetlock H (2007) The long-term effect of digital innovation on bank performance: An empirical study of SWIFT adoption in financial services. Research Policy pp: 984-1004.
64. Tetlock H, Yan J,Tayi GKJ (2008) Profiting from innovation in the digital economy: Enabling technologies, standards, and licensing models in the wireless world. Research Policy 47: 1367-1387.
65. Tendulkar R (2013) Cyber-crime, securities markets and systemic risk. CFA Digest, 43: 35-43.
66. Veronesi K (1999) Transaction management for m-commerce at a mobile terminal. Electronic Commerce Research and Applications 5: 229–245.
67. Watkins B (2014) The impact of cyber attacks on the private sector. Briefing Paper, Association for International Affair 12.
68. Wylie K (1999) Privacy, trust and policy-making: Challenges and responses. Computer Law & Security Review 25: 69-83.