Does Cyber Tech Spending Matter for Bank Stability?

Md Hamid Uddin[*]
Associate Professor of Finance
Director, PhD Program (Business)
School of Finance and Economics
Taylor's University, Malaysia.
Email: mdhamid.uddin@taylors.edu.my
iba_hu@yahoo.com

Sabur Mollah, PhD
Chair in Financial Management
Sheffield University Management School
The University of Sheffield, Sheffield
United Kingdom
Email: s.mollah@sheffield.ac.uk

Md Hakim Ali
Research Scholar
Taylor's University, Malaysia.
Email: mdhakimali@sd.taylors.edu.my

[*] This research is the output of Taylor's University's flagship research project # TUFR/2017/004/05: Cyber Risk and Bank Stability. Md Hamid Uddin is the leader, and Sabur Mollah is the external collaborator for this research project. Md Hakim Ali is working as a research scholar for this project. We acknowledge data extraction assistance received from M. Sawkat Hossain and Syed Rahman. All comments should be sent to project leader Md Hamid Uddin at mdhamid.uddin@taylors.edu.my or iba_hu@yahoo.com.

Does Cyber Tech Spending Matter for Bank Stability?

Abstract

This paper aims to investigate how digital transformation affects bank stability. This research issue is relevant because the fintech revolution during the post-financial crisis period pushes banks to embrace disruptive cyber technology more aggressively to remain competitive and retain market share. Banks improve operational speed and service quality by relying on cyber technology but expose themselves to formidable operational risks from cybersecurity hazards and systems breakdowns. However, they have no better alternative but to spend more on new technical solutions to combat technological hazards. Therefore, we examine if the law of diminishing return due to overspending on cyber technology would affect bank stability. Based on a global sample from 43 countries, we find that a marginal increase in cyber technology spending would adversely affect the stability of a bank. It is because banks take more than the proportional risk for every dollar they spend on disruptive cyber technology. While results persist across subsamples, we find two technological regimes, especially diminishing return regime can improve stability by further spending on technology aggressively and excess spending on disruptive cyber technology makes a bank more unstable in the increasing return regime.

Key words: Bank stability, Risk taking, Cyber technology, Cybersecurity, Fintech.

1. Introduction

How to maintain a stable banking system is a question for the global economies because instability in the financial sector leads to the financial crisis with detrimental effects on the economic system, affecting the allocation of resources across global economies. Therefore, researchers, regulators, and policymakers have been making efforts to understand the sources and dynamics of banking instability. The existing studies on banking stability address a wide variety of issues such as governance problems (Anginer *et al*., 2018a), regulatory weakness (Ahamed & Mallick, 2017; Cabrera *et al*., 2018), institutional supervisions (Bermpei *et al*., 2018; Shaddady & Moore, 2019), liquidity problems (Acharya & Mora, 2015), capital adequacy (Anginer *et al.*, 2018b), bank concentration and competition ((Clark *et al.*, 2018; Goetz, 2018; Fu *et al.*, 2014), and operational inefficiencies (Schaeck & Chiak, 2014), among other topics. However, there is little academic research on operational risk exposures and bank stability. The operational risk arises from the likelihood of direct or indirect losses resulting from inadequate or failed internal processes, people, systems, and external events (Basel Committee, 2010, p. 3; Basel Committee, 2011, p. 3). Although operational risks have different dimensions, the disruptive cyber technology appears to be the leading source of hazards for banking operations in the digital environment because of the impregnable cybersecurity threats. Yet, sufficient investment in cyber technology becomes a strategic necessity for the banks without regard to the concerns of security risks and investment returns because of the digital transformation of global society and post-financial crisis fintech revolution in the financial sector – affecting the earnings and market share of traditional banks (Vives, 2019; Buchak, Matvos, Piskorski, & Seru, 2018; Vives, 2019).

In this study, we investigate if cyber technology spending by banks affects their financial stability. Based on the global data, we find that a marginal increase in cyber technology spending adversely affects the stability of a bank, suggesting that banks overall take more than the proportional risk for every dollar of the spending on disruptive cyber technology. This research issue is relevant because internet has changed the paradigm of the financial industry globally as the banks and financial institutions have been increasingly offering financial services and managing internal operations in a virtual environment that becomes enormously vulnerable to cybersecurity risk. Therefore, banks have no option but to increase spending on cyber technology, often without regular capital investment analysis, to develop a more secure digital infrastructure (Kauffman *et al.*, 2015). Also, in the competitive environment, banks have no choice but to continuously improve their electronic banking system to enhance operational efficiency, performance and service quality (Roth & Jackson-III, 1995; Lages, 2016). Therefore, the banks globally have been increasing their technology budgets. According to a recent report, the global technology spending by banks will grow by 4.4% in 2019, and total spending will rise to USD309 billion by 2022 (Greer *et al*., 2019).

However, no prior study examines whether the excessive growth of cyber expenditure could affect the bank's stability. The early research finds that digitalization of financial services increases the productivity of banks (Frischtak, 1992) due to the economies of scale (Esho & Sharpe, 1995; Hancock et al., 1999) resulting from automated payment systems (Hancock & Humphrey, 1997), accelerating financial intermediation (Chemmanur, 2002). As banks are investing more on cyber technology over the last few decades, particularly in fintech era, the cybersecurity hazards are also appearing as a new challenge for the banks due to unpredictable security breaches by the external and internal agents. One study finds that cybercrime will cost around USD 6 trillion annually by 2021 (https://cybersecurityventures.com). Therefore, subsequent research suggests the scale of economies from the use of technology might be waning (Koetter & Noth, 2013) due to the economic law of diminishing marginal returns.

The diminishing returns of cyber investment is a matter of concern because of other interacting factors, such as human interaction with technology. It is a critical matter since a human has an inherent motive to gain materially by cheating if there is an opportunity (Dufwenberg & Dufwenberg, 2018, p. 263). The absence of effective control on human interaction with the cyber system leads to the rise of cybersecurity breaches. As the cybersecurity risk is a new operational problem and an effective control method is yet to be known, banks have no better option than to continuously upgrade their cyber-infrastructure with the latest secure-technology without consideration of the marginal profitability of spending. It means increases in cyber overheads beyond the threshold level may cannibalize the marginal gain of cyber spending. Therefore, optimal investment in technology with a positive net present value is a challenging matter.

Overall, we argue that bank stability would suffer if cyber technology spending goes beyond the threshold level.

For empirical testing, we gather cyber spending data for 10 years from 2008 through 2017 by manually searching a total of 3540 annual reports for 354 banks from 43 countries. The results show that cyber technology spending has a significantly concave down relationship with the banking stability, after controlling for both bank and country-level variables and unobservable country and year fixed effects. We examine two proxies of cyber technology spending: (i) natural log of the total cyber technology expense of a bank and (ii) cyber technology expenses as the percentage of non-interest operating costs. Both the measures of cyber spending consistently show a concave down effect on the financial stability, suggesting that banks can improve their stability up to the threshold level and a further increase in cyber spending affects the stability of banks adversely. The sub-sample analysis finds that cyber spending has a similar effect on the financial stability of both small and large banks, and the effect is significantly noticeable during fintech era emerged after the global financial crisis period. However, results differ depending on the technological advancement of the country. We find cyber spending yields a significantly positive linear effect on the stability of banks in those countries only where the level of technological advancement is still low. However, the positive impact of cyber spending gradually wanes as the country advances more toward the maturity level of technology use. Overall, the study confirms that banks take more than the proportional risk for every dollar they spend on the disruptive cyber technology subject to the technological regime of the country.

This study has several novel contributiont o the body of finance and banking literature. Firstly, to the best of our knowledge, this is the first rigorous research providing both theoretical analysis and empirical evidence from global data to document that increase in cyber technology spending exerts an adverse effect on the banking stability after a threshold point, manifesting the impact of diminishing returns law of economics for cyber investment by banks. Secondly, the study finds that a bank′s marginal benefit (financial stability) from cyber spending gradually wanes when the country improves its commitment toward technological advancement. Therefore, banks need to spend more aggressively on cyber technology to improve their financial stability when the country has already moved to the diminishing return regime. Overall, all banks, irrespective of size, need to be more cautious while increasing their cyber technology budget as excess spending on disruptive cyber technology decreases their financial stability. Thirdly, the fast growth of fintech over the last decade influences the traditional banks to spend more on cyber technology despite the concern of losing financial stability.

Finally, our study has both theoretical and practical implications. The results shed a different light on the argument that technology can defy the law of diminishing returns; thus, the study opens a new avenue of thinking by the theoretical researchers as the positive effects of cyber technology spending on the stability of banks diminishes after a threshold point. This finding may spur corporate finance researchers to think about the optimal threshold point for technology spending in the future. The policy makers, regulators, and banker managers can have an insightful view from this empirical study. As country advances toward the developed stage, the policymakers and regulators need focusing more on the cybersecurity governance mechanism rather than enforcing on technology solutions, and bank managers need to do a careful analysis of costs and benefits before committing to increasing their cyber technology budgets.

We organize rest of the paper in following sections: Section 2 provides the literature review and theoretical discussion on how cyber technology spending affect the stability of banks. Section 3 describes test methods and data. Section 4 presents study results and provides discussions. Finally, the conclusion is given in the last section.

2. Literature, theory insights, and hypothesis

In this section, we first briefly summarize the body of current literature answering why and how a banking institution becomes unstable, affecting the intermediation function. Then, we show how the systemic pressure from the widespread digitalization of banking system increases the need for cyber technology spending and banks' risk-taking. Next, we make efforts to understand the banking stability consequence of rising cyber technology spending from the perspective of economic and corporate finance theories. Finally, we draw the main hypothesis of the study.

2.1.1. Banking stability puzzle

The central role of a bank is maturity transformation by converting the short-term savings into long-term loans based on the assumption that most people will not withdraw all their cash at the same time. In the process, banks often slip out of the optimal risk-taking while extending credits. There is a plethora of research on the issue of why banks take excess credit risk and thereby fall into the liquidity problem leading to the instability of banks. The researchers examine the nexus of credit risk, liquidity risk, and bank stability from different perspectives and find a link between them: credit and liquidity risks interact to influence the bank stability (Wagner, 2007; Acharya & Mora, 2015; Acharya & Viswanatha, 2011; Acharya, Shin, & Yorulmazer, 2011; He & Xiong, 2012). Literature also shows that credit and liquidity risks have an individual effect, besides their common effect, on the probability of bank default (Imbierowicz & Rauch, 2014). However, the underlying mater affecting bank stability still perplexing us because other studies find that the tightening of liquidity regulation does not influence the lending behavior of the UK banks (Banerjee

& Mio, 2018), and monetary policy has a limited power in controlling bank liquidity of the US banks (Berger & Bouwman, Bank liquidity creation, monetary policy, and financial crises, 2017). The study also finds that government liquidity support in crisis does not help a bank if it has an existing solvency problem (Boyson, Helwege, & Jindra, 2014). Hence, it is broadly accepted that credit and liquidity risks are the systemic problems in the banking institution that require efficient management.

The research strand that focuses on the capital ratio and bank stability has disagreement on the appropriate bank capital structure for various reasons (Holmstrom & Tirole, 1997; Mehran & Thakor, 2011; Allen, Carletti, & Marquez, 2011; Berger & Bouwman, 2013), but all generally agree that a higher capital ratio promotes banking stability because of a reduction in the systemic risk (Anginer, Demirgüc-Kunt, & Mare, 2018b; Laeven, Ratnovski, & Tong, Bank size, capital, and systemic risk: Some international evidence, 2016). As the level of leverage of a bank affects its risk-taking incentive (Dell'Ariccia, Laeven, & Marquez, 2014) and determines the ability to withstand economic shocks, researchers have been studying the underlying reasons why a bank wants to have more or less capital buffer, and regulators focusing on the guidelines and rules to control bank capitals for the overall stability of the financial system. However, the outcomes are not always positive when regulators adjust capital requirement for the banks to stabilize the financial system (Abou-El-Sood, 2016; Bandt, 2018), as the effect of regulatory capital adjustment on the loan growth influencing credit and liquidity risks is subject to the existing level of bank capital (Deli & Hasan, 2017). Therefore, another line of research explores if the weakness in governance and regulatory supervision of banks has a role in risk-taking and stability of the banks, but results are mixed (Ahamed & Mallick, 2017; Cabrera, Gerald, & Nieto, 2018; Bermpei, Kalyvas, & Nguyen, 2018; Shaddady & Moore, 2019; Anginer, Demirguc-Kunt, Huizinga, & Ma, 2018a).

Another research string examines the influence of banking concentration and competition on the risk-taking behavior of banks and their financial stability, and again findings are inconsistent across countries. Some studies broadly find competition improves bank stability in the US, the Commonwealth of Independent States (CIS), and 14 Asia-pacific countries (Goetz, 2018; Clark, Radic, & Sharipova, 2018; Fu, Lin, & Molyneux, 2014). However, other studies find more competition instead negatively affect bank stability in the Middle East and North African (MENA) countries and other economies where both Islamic and conventional banks work alongside (Albaity, Mallek, & Noman, 2019; Azmi, Ali, Arshad, & Rizvi, 2019). Overall, the brief review of literature presented above shows that researchers have been juggling with different reasons of risk-taking by banks and their financial instability, but we are not adequately clear about the bottom of the problem: why and how a bank takes an excess risk and falls into the financial instability. The problem of banking stability has been well-studied from different perspectives, but there is little

academic research on the operational risk exposures and stability of the banks. Hence, literature in this area is yet under developed.

Basel committee defines the operational risk as to the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events (Basel Committee, 2010, p. 3; Basel Committee, 2011, p. 3). The operational risk usually incurs unwillingly due to the rise of matters affecting the internal operational processes that include, technology infrastructure, security system lapse, data loss, unexpected monetary loss, fraud, privacy protection, legal issues, operation shutdown and environmental factors, etc. It means operational risk exists as long as systems, processes, and people behave imperfectly. The broader definition of operational risk covers a myriad of risk factors, but the gravity of threats emerging from technology is well-recognized in Basel guidelines for operational risk management, as well as in the documents of International Monetary Fund (IMF), World Bank, Organization for Economic Cooperation and Development (OECD), among others agencies. Also, the country-level regulators have been issuing policy guidelines for managing the operational risk arising from cyber technology use[1]. 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. Therefore, we make efforts below to understand the channels through which cyber technology use could affect banking stability.

2.1.2. Cyber technology and banks' financial stability

Technology adoption enhances efficiency to the financial institutions and fosters financial development through enhancement of financial inclusions globally (Tchamyou, Erreygers, & Cassimon, 2019), as the financial institutions can extend financial services to the customers, including those previously unbanked, in the fastest way and cost-effectively due to innovation of the online and mobile banking platforms (Agyekum, Locke, & Hewa-Wellalage, 2016). The speed of financial inclusion has been manifested exponentially with the worldwide revolution of financial technology (Fintech) - allowing payments, saving, borrowing, and managing risk by defying the barriers (Demirguc-Kunt, Klapper, Singer, Ansar, & Hess, 2018). About the consequences of technological development in the banking sector, the early research finds that technology adoption increases the market power of a bank that enhances its profit buffers, which is useful to withstand adverse shocks. However, the bank increases the vulnerability to financial distress by choosing risky portfolios of assets and liabilities when competition increases (Koette & Poghosyan, 2009),

[1] 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.

suggesting a complex relationship bank competition and financial stability (Allen & Gale, 2004). Therefore, it is unclear if widespread application of cyber technology indeed helpful for the banks.

In this circumstance, we observe the outbreaks of cyber breaches in recent years that incur unprecedented direct financial losses by the banks globally, manifesting the vulnerability of cyber technology[2]. It happens because there are countless ways of breaking cyber system, such as unknown malware, phishing, internal and external system abuse, and targeted cyber-attacks, etc. among other ways. Therefore, the risks of cyber breaches have been emerging as the systemic hazard that may set off without a signal to create a major economic shock for the affected bank with also a contagion damaging effect across the financial system networks (Johnson, 2015; Hurd, 2016). Therefore, with the rise of cyber risk[3], it becomes an immediate necessity for the financial institutions globally building up a more resilient but efficient cyber technological infrastructure – rising capital investments in the most secure software and hardware, data encryptions, firewalls, surveillance, risk detection by artificial intelligence, human capital development in cyber technology with education and training.

However, it is appearing that cybersecurity risk becomes an impregnable hazard of the online banking system because cyber breaches are also increasing at the same pace with the advancement of technology. In this regard, the most recent study finds that the primary source of cybersecurity risk is the behavior of human, but not necessarily the hazard of technology (Eling & Wirfs, 2019). This finding suggests that excess spending on cyber technology beyond the optimal level might not help to reduce the exposure of cybersecurity risk. However, an early study finds it challenging to identify the optimal level of technology investment because the environment (technological and economic) in which firms (banks) operate has been evolving continuously toward the different levels due to the rapid technological changes and innovations superseding the existing technologies (Tang & Zannetos, 1992). Despite that the optimality of cyber technology spending is difficult to be known (Eling & Lehmann, 2018), banks have hardly any alternative choice but to increase their technology budgets to tackle the growing risk of cybersecurity. Therefore,

[2] A few examples for cybersecurity incidences: Tesco bank lost 2.5 million pounds (Treanor, 2016), Bank of Russia lost around $31 million in 2016 (Thomson Reuters, 2016). Bangladesh central bank lost US$81 million in 2016 (Gopalakrishnan & Mogato, 2016), Vietnam's Tien Phong Bank lost USD one million losses in 2015 (CNBC, 2016). Banco Del Austro in Ecuador had USD 12 million financial loss in 2015 (Finch, 2016). A cyber-crime gang named Carbanak stole one billion USD through several cyber-attacks in 2014 (Kaspersky, 2015). These are the tip of the iceberg of cybersecurity problems in the financial industry around the world.

[3] Financial Times reports that 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 (Mee & Schuermann, 2018).

banking institutions slowly enter into the vicious circle of technological dependence (Ngonzi, 2016), leading towards more risk-taking from cyber technology.

The overall banks' risk-taking including that of the cybersecurity breaches become further complicated as fintech revolution after the financial crisis changes the operational structure of the global financial market. With the rise of the regulatory burden on traditional banks after the financial crisis, the disruptive cyber technology creates the opportunities for fintech firms to enter shadow finance market - contributing to the decline of traditional banks' market share (Buchak, Matvos, Piskorski, & Seru, 2018). Basel committee on bank supervision identifies that the nature and scope of banking risks as commonly understood significantly change with the emergence of fintech because new technologies affect the traditional bank business models, leading to the enhancement of strategic and profitability risks, operational risks, cyber risks and compliance risks for the traditional banks (Basel Committee, 2018). The strategic and profitability risks occur because fintech developments lead to more competition for the traditional banks, impacting the sustainability of their earnings in the changing environment[4]. Therefore, banks are increasingly adopting advanced cyber technologies or building a partnership with fintech firms to deliver innovative financial products and services that require more investment in technologies.

As banks' strategic focus is shifting towards developing either in-house technology infrastructure or making a partnership with fintech firms[5], the business operational risk is also escalating due to increased technology interdependencies between the banks, and even between the banks and fintech firms (Härle, Havas, & Samandar, 2016). Furthermore, the proliferation of innovative products and services based on advanced cyber technology and fintech collaborations making it more difficult for the traditional bank managers to control the operational risks in the digital banking platform. The widespread technology adoption, big data analytics, and fintech partnership or outsourcing could lead to compliance risk about data privacy (Basel Committee, 2018). If technology-based banking network allows customers to switch between different banks and fintech firms to obtain a better return, the volatility of bank funding could add to credit and liquidity risk. Apart from above operational matters, increased interconnectivity between market players such as banks and fintech firms can create benefits for the institutions and customers, but cybersecurity risk also amplifies - making banking system even more vulnerable to cyber-threats. Overall, fintech revolution

[4] A recent study finds that, due to regulatory imperfection and supervision failure, fintech-driven market competition becomes detrimental to bank stability because the development of shadow banking and unregulated banking activity pervasively affecting banks' risk-taking (Vives, 2019).

[5] 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).

associated with cyber technology advancement after the financial crisis further aggravates the technology-driven risk-taking of banks, affecting the stability of banks

2.1.3. Theory insights and hypothesis

The problems associated with excess adoption of cyber technology is a growing concern for the stability of banks, but the potential benefits are also attractive because cyber technology helps the traditional banks to compete well in digitalized society by expanding financial services to the broader pool of bank customers (financial inclusion), tailoring banking services, speeding up the delivery of services through remote access, improving operational efficiency and reducing costs (FSB, 2017; Basel Committee, 2018). The recent development of regulatory technology (regteg) are also useful for the financial institutions and regulators to deal with complicated compliance processes and reduce the compliance risks arising from the adoption of cyber technology in banking services. Therefore, based on the economic law of diminishing returns, we provide theoretical insights for proceeding toward hypothesis construction. If we assume the cyber technology infrastructure is the factor playing a role in the stability of banks operating in the digitalized socio-economic environment, then the crucial question is whether spending an extra dollar for the cyber technology has a marginal benefit for the bank stability. It is a pertinent question because technology infrastructure *per se* cannot help unless cofactors such as human factor, banking regulations, governance, supervision, etc. are integrated well with the adoption and changes in cyber technology.

Our critical analysis of cyber technology and banks' financial stability presented above broadly identify that the lack of synchronization between the technological innovations and other cofactors affecting bank performance could lead to banking instability. In this case, literature shows that the human factor is responsible for cybersecurity risk (Eling & Wirfs, 2019), which appears to be an impregnable technology hazard creating shattering adverse effects on the financial industry. The banks' personnel are supposedly well-trained in banking business and operations but not in the handling and management of cyber technology. Banks do invest in human development for technology management, but they need external collaborations with the technology firms. It means banks have lesser control over the operations as they are increasingly using cyber technology and relying on the external technology firms. Also, literature shows that traditional banks are burdened with regulations after the period financial crisis period but the financial technology firms expanded their activities in the absence of adequate regulatory controls and supervisions (Buchak, Matvos, Piskorski, & Seru, 2018), and Basel Committee (2018) report suggests that future banking regulations need more alignments to bridge the gap created between the technological advancement and financial regulations. Therefore, if all cofactors affecting bank performance cannot work in tandem, it is likely that increased use of cyber technology fails to defy the economic law of diminishing returns

because the marginal gain from technology might be cannibalized due to the costs associated with the technology risks discussed earlier.

The study by Beccalli (2007) supports the above theoretical insights from the economic law of diminishing returns. Based on a sample of 737 European banks, the study finds that higher technology spending has an apparent adverse effect on profit efficiency while an unclear impact on the cost efficiency of European banks. Also, outside the developed economies, a stochastic frontier analysis finds similar profitability paradox with the increase of technology adoption in the Indian banking industry (Gupta, 2018). Hence, we conjecture that, in the digitalized socio-economic environment, technology spending becomes a strategic necessity for the banks without regard to the concern of profitability. However, it is difficult for a bank to identify the level of necessity due to the speed of changes and innovations in technology, fintech revolutions and increased market competitions, pervasive operational risks of disruptive cyber technologies influencing other risk drivers of bank, and the contingent risks of cybersecurity breaches and system breakdowns. Also, for these reasons, the conventional estimates of net present value (NPV), internal rate of return (IRR), or paybacks are also less useful for analyzing strategic capital investments in technology (Gordon & Loeb, 2002; Shank, 1996). Hence, banks have incentive to allocate sufficient budget to strategically remain at the forefront of technological changes and market competition, as well as to maintain the resiliency of the technology infrastructure from cybersecurity hazards. Therefore, from corporate finance perspective, banks take more business risk because of the uncertain marginal value addition from cyber technology spending.

Overall, the analysis and theoretical insights above suggest that the rapid development and innovation in cyber technologies over the last decade, particularly after the global financial crisis, has changed the nature of banks' risk-taking behavior - affecting the financial stability. It is because the pervasive technology hazards enhance overall operational uncertainty as banking infrastructure is more fragile due to impregnable risks of cybersecurity and system breakdown, as well as the application of disruptive cyber technology across the board and fintech revolution have contagion influence on the banks' business strategy, credit, liquidity, competition, compliance, governance, supervision, and business risk. Therefore, we argue that banks may need to have sufficient technology budget, but an excess spending on disruptive cyber technology could adversely influence the financial stability of a bank. Hence, we construct the following hypothesis.

H_A: *A marginal increase of cyber technology spending more than necessity level adversely affects the stability of a bank.*

3. Variables and test models

3.1. Dependent variable

Financial stability is a broad concept that researchers examine from different perspectives by using proxy measures suitable for the context of their studies. The stability measures also differ subject to the scope of study such as financial system stability vs. bank-level financial soundness. In this study, we examine the financial soundness of a bank to withstand economic shocks coming through different channels as the global banking sector has been transforming into a technology-driven system. Therefore, it is essential to consider whether a bank can maintain a stable flow of net earnings and build a sufficient capital buffer by increasing its spending on the disruptive cyber technology to overcome the shocks resulting from technological transformation occurring in the banking system. Therefore, we use *Z-score* estimated by $(ROA + (Equity/Assets))/\sigma ROA$ as a suitable proxy[6] measuring the financial soundness of a bank. It explicitly compares the buffers such as return on asset (ROA) and capital ratio (equity to asset) of a bank with the volatility of asset returns; thereby, measuring the solvency risk of a bank. A higher z-score implies a lower probability of insolvency as the bank maintains a steady flow of net earnings and sufficient capital buffer.

The Z-score is based on accounting data, which is the main point of criticism as the accounting practices and audit quality matter for the accounting performance. However, the study finds that $Z\text{-}$ *score* can predict about 76% of bank failure in the US (Chiaramonte, Liu, Poli, & Zhou, 2016); thereby, it is a well-accepted bank risk-taking measure in the literature (Demirgüç-Kunt, Detragiache, & Tressel, 2008; Laeven & Levine, 2009; Čihák & Hesse, 2010; Beck, Demirguc-Kunt, & Merrouche, 2013). Since this Z-score uses the after-tax return on assets, we cannot exclude the contribution of the country's tax environment to the financial stability of a bank. Therefore, for robustness checking, we re-estimate it based on the income before taxes. The re-estimation of a Z-score after excluding the effect of taxes helps us to better understand the managers' contribution to the financial stability of a bank. In the literature, we find researchers have used corporate risk-taking proxies based on the operating income instead of the net income after taxes (Boubakri, Cosset, & Saffar, 2013; Faccio, Marchica, & Mura, 2011).

[6] We find studies use market-based distance-to-default (DD) based on the option pricing framework to estimate the probability of default - assuming that total equity capital is a buffer against the default. However, the regulator takes action before a bank reaching to the level of default point; it means default may not occur in reality. The DD estimation also assumes that all debts retire in one year, which is not realistic. However, DD is useful for bank rating purpose. Financial stability of banks can be measured in CAMELS framework, applying suggested score for the component ratios based on Basel guidelines as well as local regulatory requirements. It is generally used as a bank supervision tool. The value-at-risk and expected shortfall are two risk measures that determine bank stress level and the capital requirement to absorb economic shocks, hence, these are useful for bank regulators. Overall, these measures are less useful for our study because we examine whether a bank can maintain steady flow earnings and capital buffer with the changes in the level of cyber technology spending.

3.2. Independent variables

3.2.1. Focused variables

We create two variables to capture the effect of cyber technology spending on bank stability. These are the natural log of total cyber technology spending (*CyberTech-1*) and total cyber technology spending as the percentage of non-interest operating expenses (*CyberTech-2*). The cyber technology spending includes all kinds of costs related to software, hardware, data processing, outsourced technology supports, staff training on cyber technology matters, etc. Of these, *CyberTech-1* is an aggregate measure transformed into the natural log, while *CyberTech-2* is the relative measure of cyber technology spending. Both measures of cyber technology spending have academic and practical significance. The aggregate measure *CyberTech-1* provides an idea about the overall technology budget of a bank because it is a strategic budgetary allocation while the relative measure *CyberTech-2* gives an idea about the bank's policy on technology vs. non-technology expenses. Since our hypothesis imply a concave downward relationship between the cyber technology spending and bank stability requiring us to test non-linear models, we also create squared variables such as *CyberTech-1 squared* and *CyberTech-2 squared*.

To construct *CyberTech-1* and *CyberTech-2*, we hand collect relevant data by manual searching of 10 years' annual reports of 354 banks belonging to 43 countries. As there is no mandatory requirement yet to disclose technology expenses separately in the bank financial statements, we apply a systematic approach to manually search annual reports of our sample banks. Firstly, we check the income statement if bank reports technology expenses under the heading of 'technology expense' or any related term such as IT expense, ICT expense, etc. Secondly, we carefully review the detailed breakdown of non-interest expense figures reported in income statement that are available in the end-of-statement notes. We do this search to identify if any sub-item of the total non-interest expense relates to the cyber technology spending. Thirdly, we review the detailed breakdown of depreciations and amortizations for intangibles asset to identify of any component of depreciations and amortizations related to hardware and software. Finally, we compile and reconcile the data collected from annual reports to construct two focused variables.

3.2.2. Bank-level controls

Following the literature, we select (i) total asset, (ii) asset turnover, (iii) cost-to-income ratio, (iv) interest margin, (v) tier-1 capital ratio, (vi) equity-to-asset, and (vii) non-performing loans as the bank-level control variables for empirical tests. *Total Assets* is the common bank-level control that is widely used by the most previous studies because financial soundness of banks varies with the size of bank assets. Haan & Poghosyan (2012, p. 3009) provides a summary of previous studies on the relationship between

bank size and bank risk. *Asset-turnover* ratio directly determines the return on assets through Du-Pont identity and shows the risks of assets choices of a bank affecting the financial soundness (Wagner, 2007). *Cost-to-income* ratio determines the level of bank efficiency influencing the stability (Schaeck & Chiak, 2014). *Interest margin* determines the ability of a bank to manage interest rate risk that impacts bank profitability (Chaudron, 2018). The effect of capital ratio on bank stability is well-established in the literature, and the recent study finds bank capital is associated with a reduction in the systemic risk contribution of individual banks in the system-wide fragility (Anginer, Demirgüc-Kunt, & Mare, 2018b). Therefore, we include *tier-1* capital and *equity-to-asset* ratios as the controls for bank capitals. Finally, we take the percentage of the *non-performing loan* as another important bank-level variable directly affecting the financial soundness of a bank. Nikolopoulos & Tsalas (2017) provide a review of the literature on loan performance and its impact the bank performance.

3.2.3. Country-level controls

As our sample includes global data, we identify a set of country-level controls variables that are relevant for this study. These include (i) cybersecurity commitment, (ii) corruption, (iii) financial freedom, (iv) gross domestic product, and (v) inflation. *Cybersecurity commitment* is the score awarded to a country by the International Telecommunication Union (ITU) based on the country-level policies and mandatory regulatory requirements to build up a resilient cyber society. Therefore, we assume the level of a country's commitment to resilient cyber society would affect the budgetary allocation of a bank for cyber technology spending. *Corruption* variable is the corruption perception score of a country as reported by Transparency International, which ranges from 0 (highly corrupt) to 100 (very clean). About corruptions in the country, the literature finds that banks extend credits without adequate risk assessment based on the political considerations, and such corrupt practices escalate loan defaults affecting the stability of banks (Infante & Piazza, 2014). *Financial freedom* is the financial freedom index of a country provided by Heritage.org. We take this variable because study finds that higher financial freedom in the economy promotes the level of banking efficiency (Chortareas, Girardone, & Ventouri, 2013). *Gross domestic product* is the natural log of the real gross domestic product (GDP) per capita of the country denominated in USD. Evidence shows that GDP influences banking performance through monetary policy shocks (Jiménez, Ongena, Peydró, & Saurina, 2012). *Inflation* is the annual rate of inflation of a country measured consumer price index, and

evidence shows that inflation affects (Boyd, Levine, & Smith, 2001) the lending activities and financial market performance of a country (Boyd, Levine, & Smith, 2001).

3.2.4. Fixed effect control

As the study uses multi-country data for 10 years, we apply a country-year interaction (*Country*Year*) variable to capture the effects of unobservable country-level common factors on the performance of a bank in a particular year operating in the country. In an earlier study for bank performance, Beck, Demirguc-Kunt, & Merrouche (2013) have used this interaction variable. We apply this variable in ordinary least squared (OLS) estimation.

3.3. Test models and estimations

We specify following base model for empirical test:

$$Bank\ stability_{it} = \alpha + \beta_i CyberTech_{it} + \sum_{i=1}^{N} \gamma_i Controls_{it} + \varepsilon_i \quad (1)$$

Where $Bank\ stability_{it}$ is *Z-score* of the bank *i* for the year *t*. $CyberTech_{it}$ is the measure of cyber technology spending by the bank *i* for the year *t*. We test two alternative measures of cyber technology spending such as *CyberTech-1* (the natural log of total cyber technology spending) and *CyberTech-2* (total cyber technology spending as the percentage of non-interest operating expenses). $Controls_{it}$ are the bank- and country-level control variables as well as the country and year interaction variable as discussed above. The summary of all test variables is available in Appendix 1. We estimate above base model in three ways. Firstly, we estimate OLS models, correcting the standard errors for country and year clustering. Secondly, we test the dynamic system GMM models by including the lag dependent variable in the model, which potentially corrects endogeneity issues and also provide more consistent estimates of the parameters. Thirdly, we run fixed effect panel regression models that supposedly corrects omitted variable bias. Overall, we can draw a firm inference about our hypothesis if the findings of base model are consistent across all estimation approaches.

4. Sample and data

As there is no regulatory requirement to disclose cyber technology cost as a separate item in bank income statements, the information is currently unavailable in the standard databases. Therefore, we manually collect cyber technology expenses data by reviewing carefully the cost items reported in the financial statements of banks. We gather the annual reports of banks from different countries following a systematic approach. First, we take countries that represent different regions of the world such as North America, Europe, Latin America, Asia, Pacific, Middle East and North Africa (MENA), and BRICS. Second, we get

the names of exchange-listed banks, then download their annual reports from the bank websites or stock markets. We can successfully download the annual reports of 354 banks from 43 countries for ten years from 2008 to 2017. We need to exclude many banks due to missing reports, or they are published in the non-English language. After reviewing all annual reports, we find a total of 264 banks disclose cost information related to cyber technology (more details in section 3.2.1) for a minimum of three years. Therefore, we get a total of 2156 data observations for cyber technology spending by banks. Overall, the sample is widely distributed across the developed and developing countries as well as different regions. The highest number of 292 observations (13.49%) are from the US market, and the lowest 21 observations (0.97%) are from Israel. The sample distribution shows the maximum 30 banks (11.36%) are from the US, and a minimum of 3 (1.14%) banks are from respectively Chile, Finland, Japan, Mexico, Netherlands, Singapore, and the UAE. Therefore, the sample and data observations of cyber technology spending represent the global view fairly. We collect the remaining data (other than cyber technology cost) from Bloomberg database. Table 9 below provides more details of the sample and observations.

[Insert Table 1]

The descriptive statistics of variables in Table 2 show that the dependent variable *Z-score* varies from -1.719 to 48.795 with an average value of 7.511 and standard deviation of 8.917. The *Z-score* (before tax), which is based on operating income before taxes, also show similar variation with a lower average of 6.438. The distributions of both *Z-scores* are skewed towards the right and leptokurtic, suggesting the existence of outliers. We find the distribution of cyber technology spending variable *CyberTech-1* is relatively normal as its skewness is (-0.318) closer to zero while kurtosis (2.983) is very close to 3.0. The distribution of *CyberTech-1 squared* is also slightly asymmetric as skewness (1.22) is marginally above one, while kurtosis (3.861) is also marginally more than 3.0. The distribution of another cyber technology spending variable *CyberTech-2* is skewed to the right side with leptokurtic peak. Also, the distributions of bank-level control variables are generally skewed towards the right with leptokurtic peaks. However, country-level controls are slightly skewed (- or +) from the symmetrical position mostly platykurtic peaks. As a whole, the descriptive statistics show significant variation in data observations with skewed distributions and leptokurtic or platykurtic peaks. It is a common phenomenon in a real-life situation. Therefore, we winsorize data observations at one percent level on both sides of the distributions, and rely on the robust *t-values* for testing statistical significance of the estimates of model coefficients.

[Insert Table 2]

5. Results and discussions

We first visualize global data to get a general idea of the relationship between cyber technology spending and banking stability measure. Then we report empirical tests results based on comprehensive global data to confirm if cyber technology spending overall affects banks' risk-taking and stability. Next, we present the results of the subsamples that are relevant in the context of the study. Then, we check the robustness of overall findings based on the alternative measures of dependent and independent variables followed by a country analysis that shows the variations of findings across countries. Finally, we provide findings insight from academic and practical perspectives.

5.1. Data visualization

As we hypothesize a marginal increase of cyber technology spending more than necessity level would adversely affect the stability of a bank, a nonlinear downward quadratic relationship between cyber technology spending and bank stability is generally expected. Therefore, we first visualize the scatter plots and polynomial regression splines of tests data in Figure 1. Based on the scatter plot, Figure 1.a visualizes a probable nonlinear relationship between the natural log of total cybertechnology spending and bank stability measure of Z-score as the scatter dots are less concentrated in the edges. The regression spline in Figure 1.b confirms a concave downward relationship between the log of cyber technology spending and *Z-score*. Figure 1.c and 1.d display a similar concave downward relationship between cyber technology spending as the percentage of non-interest operating expense and bank stability measure. Overall, data visualizations are consistent with the argument that a bank has no marginal benefit if it overspends in cyber technology despite that technology and innovations are advancing at a much faster speed.

[Insert Figure 1]

5.2. Baseline results

Table 3 presents OLS and dynamic system GMM results of the base regression for both linear and nonlinear effects of the log cyber technology spending (*CyberTech-1*) on the bank stability variable, *Z-score*. The findings of both OLS (Model-2) and GMM (Model-4) regressions show that cyber technology spending has a statistically significant nonlinear downward quadratic effect on a bank's risk-taking behavior, and thereby affecting its financial stability. The relationship between cyber technology spending and bank stability appears to be a concave down shape because both OLS and GMM coefficients for *CyberTech-1* and *CyberTech-1 squared* are respectively positive and negative, and also statistically significant. The OLS coefficients of *CyberTech-1* and *CyberTech-1 squared* are respectively 0.799 and -0.107, which are significant at the 1% level. The GMM coefficients of *CyberTech-1* and *CyberTech-1 squared* are respectively 3.144 and -0.372, which are significant at the 5% level. Overall, the nonlinear effect of cyber

technology spending on a bank's risk-taking is consistent for both OLS and GMM estimations. However, the linear tests provide inconsistent findings as OLS (Model-1) coefficient of *CyberTech-1* is insignificant while that of GMM (Model-3) estimate is marginally significant at the 10% level.

[Insert Table 3]

The findings overall support our hypothesis contending that overspending on cyber technology has no marginal benefit as it may be detrimental to the bank's financial stability due to excessive risk-taking. Therefore, our baseline results suggest that banks should be cautious while investing in technology due to the existence of hype-cycles in technological innovations (Lente, Spitters, & Peine, 2013; Dedehayir & Steinert, 2016). A bank could burden itself by quickly adopting new technology as the majority of technological innovations fail to sustain in the long run due to the existence of shorter hype-cycles. It is because the latest software and hardware could become obsolete quickly with the arrival of innovations before the current investment pays off. It is also essential to consider that the risk of a cybersecurity breach and system breakdown is not impregnable by any better technology, and customers might have difficulty in switching to new technology more frequently. In a nutshell, we show that one percent increase of cyber technology expense leads to more than one percent risk-taking by a bank.

As it is evident that banks' risk-taking is more than the proportional for every dollar they spend on cyber technology, an important question is whether banks should strike a balance between technology and non-technology expenses. Therefore, we examine the effect of cyber technology spending as the percentage of non-interest operating costs (*CyberTech-2*) on the stability of a bank. We find a similar nonlinear downward quadratic effect on the *Z-score*, based on OLS (Model-2) and dynamic system GMM (Model-4) results in Table 4. It shows both OLS and GMM coefficients for *CyberTech-2* and *CyberTech-2 squared* are respectively positive and negative. The OLS coefficients of *CyberTech-2* and *CyberTech-2 squared* are respectively 0.171 and -0.005, which are significant at the 5% level. However, the GMM estimates of *CyberTech-2* and *CyberTech-2 squared* are respectively 0.557 and -0.012. Of which, the coefficient of *CyberTech-2* is significant at the 5% percent level while that of *CyberTech-2 squared* is significant at 10%. Hence, both OLS and GMM results confirm that a concave down relationship between *CyberTech-2* and *Z-score* does exist as well. We also find that the results of linear models (Models 1 and 3) are consistently significant for both OLS and GMM estimations. Based on the linear and non-linear results in Table 4, we can suggest that banks should maintain an optimal balance of cyber technology spending as a part of total non-interest operating cost to achieve the maximum financial stability.

[Insert Table 4]

Finally, in Table 5, we present further results based on fixed-effect panel regressions that reconfirm the existence of a highly significant concave downward relationship between both measures of cyber technology spending (*CyberTech-1* and *CyberTech-2*) and bank stability (*Z-score*) due to the more than proportional increase in risk-taking for one-dollar additional expense for cyber technology. The nonlinear Model 2 finds the coefficients of *CyberTech-1* and *CyberTech-1* squared variables are respectively positive and negative; both coefficients are significant at less than 1% percent level. Likewise, Model 4 identifies the coefficients *CyberTech-2* and *CyberTech-2* squared are also respectively positive and negative with the level of significance similarly at less than 1% percent. As expected, the results of linear regressions (Model-1 and Model-2) are statistically insignificant, but the nonlinear results (Model 2 and Model 4) are highly significant. Therefore, the findings of OLS, GMM, and fixed-effect panel regressions reported in tables 3, 4, and 5 provide clear global evidence to support our hypothesis. Thereby, the empirical tests prove that a marginal increase in cyber technology spending more than necessity level would adversely affect the stability of a bank. Next, we undertake a subsample analysis of results across different dimensions that are relevant for this study.

[Insert Table 5]

5.2.1. Bank sizes and financial stability

The technology policy and strategy of banks could differ subject to the availability of resources, and industry analysts find that retail banks struggle to face the most challenges of the digital era due to limited resources while the large banks can dedicate more funds on developing digital infrastructure to combat cybersecurity threats and compete with the fintech firms. Also, the prior studies find the bank stability varies with bank sizes and their market shares (Pawlowska, 2016; Kim, Park, & Song, 2016). Hence, we examine if cyber technology spending by small and large banks have a different impact on their financial stability. For empirical testing, we classify the samples into small and large banks. The small banks are those with total asset below the median value while the large banks are those with asset value above the median. The regression results in Table 6 generally show cyber technology spending has a significant nonlinear quadratic effect on the stability of both small and large banks, as the results of nonlinear models (Model 2 and Model 4) are significant while those of the linear models (Model 1 and Model 3) are insignificant. These findings suggest the pervasiveness of technology risks, as it adversely affects the stability of all banks irrespective of their size because every dollar spending on cyber technology leads to more than proportional risk-taking by a bank. Hence, our results differ from earlier studies that find banks' riskiness vary with the bank sizes (Varotto & Zhao, 2018; Laeven, Ratnovski, & Tong, 2016), as results show the size of the banks does not matter if banks take due to the overspending on cyber technology.

[Insert Table 6]

5.2.2 Technological advancement and financial stability

We assume that country-level development of cyber technology adoption and maintenance of a resilient cyber-infrastructure could play a role in banks' decision of technology spending. If the country has a strong commitment to the technological transformation of the society and has developed policy frameworks and regulatory requirements to build a nation-wide resilient cyber-infrastructure by using the latest and hybrid technologies, then banks need to comply with regulatory requirements concerning technology adoption and cyber-infrastructure maintenance (Crisanto & Prenio, 2017). The International Telecommunication Union (ITU) periodically assess[7] the commitment level of a country to build a cyber-resilient nation and give an aggregate score based on several criteria such as ICT regulations, technical infrastructures, organizational development for implementing ICT initiatives, national level capacity building programs, cooperation with local and international agencies. Based on ITU assessment scores, we classify sample countries into three groups: (i) initiating level, (ii) maturing level, (iii) leading level. The initiating level countries are those with a cyber resilience commitment score below the 33rd percentile; the maturing level countries are those with a score between the 34th and 67th percentiles, and the leading countries those with a score above the 67th percentile. The empirical findings in Table 7 show that marginal benefit of cyber technology for banking stability gradually wanes as the country moving out from the initiating level and gradually reaching to maturity in technology adoption and cyber resiliency.

[Insert Table 7]

We find that the linear model (Model 1) coefficient of *CyberTech-1* is significantly positive in the initiating level countries, suggesting that banks of these countries can improve performance by spending more on cyber technology. We confirm it because the coefficients of nonlinear equations (Model 2) are insignificant. It is because technology substitution of the manual process helps them to reduce operational costs while their technology risks are still low as the cyber penetration is yet negligible in the initiating level countries. In the maturing level countries, the linear model (Model 3) coefficient of *CyberTech-1* is still significantly positive, while the nonlinear model (Model 4) coefficients of *CyberTech-1* and *CyberTech-1 squared* appear to be significantly positive and negative respectively. It suggests the pervasive technology risks gradually to take a toll on bank performance leading to more risk-taking in the maturing level countries. When a country reaches the leading level of technological advancement, we find a marginal increase in cyber technology spending only adversely affects the stability of a bank. We confirm it because *CyberTech-1* coefficient for the linear model (Model 5) is turned into significantly negative for the banks operating in technologically leading countries. For the nonlinear model (Model 6), we find the coefficients of both

[7] The first report published in 2015 based on prior years' data and subsequent reports published in 2017 and 2019.

CyberTech-1 and *CyberTech-1 squared* are negative. Of which, *CyberTech-1 squared* is significantly negative at the less than 1% level.

5.2.3 Fintech era and financial stability

The technological transformation in the banking sector starts many years ago, but the rise of fintech firms and shadow banking after the global financial crisis changes the operational structure and market players of the global financial market over the decade. Therefore, banks have no choice but to adopt advanced technologies aggressively or build a partnership with fintech firms to retain market share and survival. Hence, we separately check the effect of cyber technology spending on the banks' risk-taking and stability during the post-crisis period fintech era. In Table 8, the results of linear tests (Model 1 and Model 3) are insignificant for both pre-fintech and fintech periods, but the nonlinear tests (Model 2 and Model 4) identify a significantly downward quadratic relationship between cyber technology spending and the banks' stability during the post-crisis fintech period. The nonlinear coefficients of *CyberTech-1* and *CyberTech-1 squared* are respectively positive and negative, and both are significant at less than the 1% level. The significantly positive coefficient of *CyberTech-1* in the post-crisis fintech period indicates that banks could have taken advantage of cyber technology to stay competitive in the market and overcome fintech challenges, yet overspending on technology leads a bank to take more risks than benefits, affecting the stability of bank negatively. The quadratic effect of technology spending on bank stability is also evident in the pre-fintech period, but the coefficient of *CyberTech-1* is insignificantly positive, suggesting the financial crisis meltdown during 2008 and 2009 takeaways technological gains as well. The adverse effect of overspending on technology is clearly noticeable in the fintech era as the *CyberTech-1 squared* is significantly negative.

[Insert Table 8]

5.3. Robustness checks

In the above analysis, we use after-tax ROA to estimate *Z-score* as the dependent variable. It means, our bank stability measure in the earlier tests is subject to the tax regulations of a country. Therefore, we re-estimate the base model by applying a *Z-score* (before tax) to exclude the contribution of the country's tax environment to the financial stability of a bank. We test both linear and nonlinear models to check if the effect of cyber technology spending on the before-tax *Z-score* is consistent with that is based on an after-tax estimation of *Z-score*. The results in Table 9 (Panel A) show that both measures of cyber technology spending (*CyberTech-1* and *CyberTech-2*) have a similar nonlinear downward quadratic effect on the before-tax *Z-score*. Overall, the results based on before-tax *Z-score* are consistent with those based on after-tax Z-score estimates as reported and analyzed earlier. Therefore, our robust tests confirm that the effect of

cyber technology spending on bank stability is not sensitive to the differences in the tax policies across countries.

[Table 9]

In earlier regressions, we test *CyberTech-1* and *CyberTech-2* as alternative proxy measures for the cyber technology spending of a bank. We include them in the regression testing as continuous variables. Of these, *CyberTech-1* finds that one percent increase of cyber technology expense leads to more than proportional risk-taking by a bank while *CyberTech-2* identifies that banks take more risk and become unstable if they spend more on cyber technology and cannot maintain an optimal balance between technology and non-technology expenses. These findings imply that banks that overspend on cyber technology are more unstable than those spending less on technology. Therefore, we split the samples into three groups based on their annual spending on cyber technology. The high technology spending banks ($CyberTech_{High}$) are those with a total yearly spending amount is greater than th75th percentile. The low technology spending banks ($CyberTech_{Low}$) are those with an annual total spending amount is lower than th25th percentile. The other banks with technology spending between the 25th and 75th percentiles are considered as the base group. Then we change the base regression by replacing continuous measures of cyber technology spending with two dummy variables:

$$Bank\ stability_{it} = \alpha + \beta_1 CyberTech_{High} + \beta_2 CyberTech_{Low} + \sum_{i=1}^{n} \Upsilon Control_{it} + + \varepsilon_{it} \quad (2)$$

In this test, $CyberTech_{High}$ and $CyberTech_{Low}$ determine the variation of bank stability due to more or less spending on cyber technology relative to the average technology cost of a bank belong to the base group. The results in Table 9 (Panel B) identify that the coefficient of $CyberTech_{High}$ is significantly negative for both after-tax and before-tax estimation of *Z-scores*, suggesting that a bank overspending on cybertechnology is less stable than the base group banks that spend moderately on technology. We find the coefficient of $CyberTech_{Low}$ is positive for both measures of Z-score, but they are insignificant. It means spending less on technology has no significant marginal benefit than spending moderately. Overall, the robust tests with dummy specifications of focused explanatory variable revalidate our earlier findings that overspending on cyber technology leads to higher risk-taking and more instability of banks, and maintaining an optimal balance between the technology and non-technology expense is essential.

5.4. Findings by region and country

Finally, we provide more insights into the above findings by presenting the result by regions and countries. We test the base regression for every country and region separately by using the alternative measures of dependent and focused independent variables. As findings are generally consistent, we discuss the results that are based on before-tax *Z-score* and *CyberTech-2*. Table 10 shows that cyber technology spending has

a nonlinear but quadratic downward effect on the bank stability in all regions of the world; however, the impact is significant mainly in North America, Europe, and MENA regions. It means all parts of the world are maturating in technology use; thus, the marginal benefit from technology spending is waning due to the economic law of diminishing returns. However, the country level findings show the different nature of the relationship between technology spending and banking stability. We find a wide variation in the country-level results. For example, banks in Germany, Greece, Netherlands, Finland, Denmark, Bangladesh, Turkey, and Argentina seem to be able to overcome the diminishing return law by more aggressive spending on technology, as *CyberTech* is negative but *CyberTech squared* is significantly positive. In the countries such as Canada, France, Belgium, Italy, Switzerland, Sweden, Indonesia, Singapore, New Zealand, Brazil, and Saudi Arabia, banks can benefit from spending more on cyber technology yet the marginal gain is not enough to resist the law of diminishing return. In these countries, *CyberTech* is negative and *CyberTech squared* is positive but insignificant. In the remaining countries including the USA, an increase in technology spending by banks still yields a positive result up to a point, but spending more than necessity point (threshold) affects the banks adversely, as *CyberTech* and *CyberTech squared* are respectively positive and negative in these counties.

[Insert Table 10]

Overall, in 19 countries, the stability of banks decline to a certain point with every dollar of technology spending followed by an improvement of stability with a further increase in technology expenditure. However, in the remaining 24 countries, an additional dollar of technology expense improves bank stability initially up to a threshold level followed by a decline in stability with more technology spending beyond the optimal level. Therefore, we find two technological regimes globally for banks' risk-taking and stability across both developed and developing countries. In one technological regime, banks would require more aggressive spending on technology to improve their performance further and overcome diminishing returns of cyber technology. In another regime, banks need to be more cautious for increasing technology expense because excess spending may lead to the stage of diminishing returns quickly. Future research can study how changes in cyber technology regimes would affect the performance and stability of banks globally.

6. Conclusion

The fast development of cyber technology changes the paradigm of the global financial industry over the last few years, as banks are offering financial services and managing operations in a virtual environment to keep pace with the digital transformation of the broader society. Digital banking has increased the speed of operations and quality of services, but banks are exposing to more operational risks due to dangerous cybersecurity hazards and unexpected system breakdowns. Moreover, disruptive cyber technology creates enormous opportunities for fintech firms to enter the shadow finance market, creating a further challenge

for traditional banks. Therefore, we study a fundamental question of whether banks are taking more risk than they spend on cyber technology by focusing it from the perspective of diminish return theory. We argue that technology alone cannot work well unless the cofactors such as human, regulation, governance, supervision, etc. are integrated successfully with the speed of technological innovations. Hence, the cost of technology risks might cannibalize the marginal return of cyber technology spending. It means an optimal technology investment for the banks with a positive net present value is a challenging matter from the corporate finance perspective.

The empirical study, based on 10 years′ data from 43 countries, finds that a marginal increase in cyber technology spending more than necessity level adversely affecting the stability of a bank because one percent increase of cyber technology expense leads to more than proportional risk-taking by a bank. We confirm it based on different estimation methods and alternative measures of the dependent and independent variables. While technology risk for the stability of banks is pervasive across the small and large banks, the effect is more noticeable in the technologically advanced countries and during the post-financial crisis fintech era. Finally, results show two technological regimes for bank stability across both developed and developing countries. In one regime, banks are likely to overcome the current diminishing return stage by more aggressive spending on technology and improve their stability. However, in another regime, aggressive cyber technology spending might lead to the stage of diminishing return quickly to adversely affect the stability of banks. Future study can further investigate how the same technological regime could persist for both developed and developing countries similarly affecting the stability of banks. Overall, three takeaways from this study. First, cyber technology spending has a nonlinear quadratic down effect on the bank stability due to diminishing return principle. Second, subject to the technological regime, a bank would decide whether to take an aggressive or softer approach for spending on cyber technology. Third, the corporate decision on a bank′s cyber technology spending need to take into the consideration of fintech challenges in the industry.

References

Abou-El-Sood, H. (2016). Are regulatory capital adequacy ratios good indicators of bank failure? Evidence from US banks. *International Review of Financial Analysis, 48*, 292-303.

Acharya, V. V., & Mora, N. (2015). A Crisis of Banks as Liquidity Providers. *The Journal of Finance, 70*(1), 1-43.

Acharya, V. V., & Viswanatha, S. (2011). Leverage, Moral Hazard, and Liquidity. *The Journal of Finance, 66*(1), 99-138.

Acharya, V. V., Shin, H. S., & Yorulmazer, T. (2011). Crisis Resolution and Bank Liquidity. *The Review of Financial Studies, 24*(6), 2166-2205.

Agyekum, F., Locke, S., & Hewa-Wellalage, N. (2016). Financial Inclusion and Digital Financial Services: Empirical evidence from Ghana. *MPRA Paper 82885*. University Library of Munich, Germany.

Ahamed, M. M., & Mallick, S. (2017). Does regulatory forbearance matter for bank stability? Evidence from creditors' perspective. *Journal of Financial Stability, 28*, 163-180.

Albaity, M., Mallek, R. S., & Noman, A. H. (2019). Competition and bank stability in the MENA region: The moderating effect of Islamic versus conventional banks. *Emerging Markets Review, 38*, 310-325.

Allen, F., & Gale, D. (2004). Competition and Financial Stability. *Journal of Money, Credit and Banking, 36*(3), 453-480 .

Allen, F., Carletti, E., & Marquez, R. (2011). Credit Market Competition and Capital Regulation. *The Review of Financial Studies, 24*(4), 983-1018.

Anginer, D., Demirgüc-Kunt, A., & Mare, D. S. (2018b). Bank capital, institutional environment and systemic stability. *Journal of Financial Stability, 37*, 97-106.

Anginer, D., Demirguc-Kunt, A., Huizinga, H., & Ma, K. (2018a). Corporate governance of banks and financial stability. *Journal of Financial Economics, 130*(2), 327-346.

Azmi, W., Ali, M., Arshad, S., & Rizvi, S. A. (2019). Intricacies of competition, stability, and diversification: Evidence from dual banking economies. *Economic Modelling*, In press.

Bandt, O. d. (2018). Optimal capital, regulatory requirements and bank performance in times of crisis: Evidence from France. *Journal of Financial Stability, 39*, 175-186.

Banerjee, R. N., & Mio, H. (2018). The impact of liquidity regulation on banks. *Journal of Financial Intermediation, 35*, 30-44.

Basel Committee. (2010). *Sound Practices for the Management and Supervision of Operational Risk.* Basel, Switzerland: Bank for International Settlements. Retrieved from https://www.bis.org/publ/bcbs183.pdf

Basel Committee. (2011). *Principles for the Sound.* Basel, Switzerland: Bank for International Settlements. Retrieved from https://www.bis.org/publ/bcbs195.pdf

Basel Committee. (2018). *Cyber-resilience: Range of practices.* Basel, Switzerland: Bank for Internattional Settlements. Retrieved from https://www.bis.org/bcbs/publ/d454.pdf

Basel Committee. (2018). *Sound practices: fintech implications for banks and supervisors.* Basel, Switzerland: Bank for International Settlements. Retrieved from https://www.bis.org/bcbs/publ/d431.pdf

Beccalli, E. (2007). Does IT investment improve bank performance? Evidence from Europe. *31*(7), 2205-2230.

Beck, T., Demirguc-Kunt, A., & Merrouche, O. (2013). Islamic vs. conventional banking model: Business model, efficicency and stability. *Journal of Banking & Finance, 37*(2), 433-447.

Berger, A. N., & Bouwman, C. H. (2013). How does capital affect bank performance during financial crises? *Journal of Financial Economics, 109*(1), 146-176.

Berger, A. N., & Bouwman, C. H. (2017). Bank liquidity creation, monetary policy, and financial crises. *Journal of Financial Stability, 30*, 139–155.

Bermpei, T., Kalyvas, A., & Nguyen, T. C. (2018). Does institutional quality condition the effect of bank regulations and supervision on bank stability? Evidence from emerging and developing economies. *International Review of Financial Analysis, 59*, 255-275.

Boubakri, N., Cosset, J.-C., & Saffar, W. (2013). The role of state and foreign owners in corporate risk-taking: Evidence from privatization. *Journal of Financial Economics, 108*, 641-658.

Boyd, J. H., Levine, R., & Smith, B. D. (2001). The impact of inflation on financial sector performance. *Journal of Monetary Economics, 47*(2), 221-248.

Boyson, N., Helwege, J., & Jindra, J. (2014). Crises, Liquidity Shocks, and Fire Sales at Commercial Banks. *Financial Management, 43*(4), 857-884.

Buchak, G., Matvos, G., Piskorski, T., & Seru, A. (2018). Fintech, regulatory arbitrage, and the rise of shadow banks. *Journal of Financial Economics, 130*(3), 453-483.

Cabrera, M., G. P., & Nieto, M. J. (2018). The G-20's regulatory agenda and banks' risk. *Journal of Financial Stability, 39*, 66-78.
Chaudron, R. F. (2018). Bank's interest rate risk and profitability in a prolonged environment of low interest rates. *Journal of Banking & Finance, 89*, 94-104.
Chemmanur, T. J. (2002). New Technologies, Financial Innovation, and Intermediation. *Journal of Financial Intermediation, 11*(1), 2-8.
Chiaramonte, L., Liu, F. H., Poli, F., & Zhou, M. (2016). How Accurately Can Z- score Predict Bank Failure? *Financial Markets, Institutions & Instruments, 25*(5), 333-360.
Chortareas, G. E., Girardone, C., & Ventouri, A. (2013). Financial freedom and bank efficiency: Evidence from the European Union. *Journal of Banking & Finance, 37*(4), 1223 -1231.
Čihák, M., & Hesse, H. (2010). Islamic banks and financial stability: An empirical analysis. *Journal of Financial Services Research, 38*(2-3), 95–113.
Clark, E., Radic, N., & Sharipova, A. (2018). Bank competition and stability in the CIS markets. *Journal of International Financial Markets, Institutions & Money, 54*, 190-203.
CNBC. (2016, May 15). Vietnam's Tien Phong Bank says it was second bank hit by SWIFT cyberattack. CNBC: Tech - Cybersecurity. Retrieved from https://www.cnbc.com/2016/05/15/vietnams-tien-phong-bank-says-it-was-second-bank-hit-by-swift-cyber-attack.html
Crisanto, J. C., & Prenio, J. (2017). *FSI Insights on policy implementation No 2: Regulatory approaches to enhance banks' cyber-security frameworks.* Basel, Switzerland: Financial Stability Institute - Bank for International Settlements.
Dedehayir, O., & Steinert, M. (2016). The hype cycle model: A review and future directions. *Technological Forecasting and Social Change, 108*, 28-41.
Deli, Y. D., & Hasan, I. (2017). Real effects of bank capital regulations: Global evidence. *Journal of Banking and Finance, 82*, 217-228.
Dell'Ariccia, G., Laeven, L., & Marquez, R. (2014). Real interest rates, leverage, and bank risk-taking. *Journal of Economic Theory, 149*, 65-99.
Demirgüç-Kunt, A., Detragiache, E., & Tressel, T. (2008). Banking on the principles: Compliance with Basel Core Principles and bank soundness. *Journal of Financial Intermediation, 17*(4), 511-542.
Demirguc-Kunt, A., Klapper, L., Singer, D., Ansar, S., & Hess, J. R. (2018). *The Global Findex Database 2017 : Measuring Financial Inclusion and the Fintech Revolution (English).* Washington, D.C.: World Bank Group.
Drasch, B. J., Schweizer, A., & Urbach, N. (2018). Integrating the 'Troublemakers': A taxonomy for cooperation between banks and fintechs. *Journal of Economics and Business, 100*, 26-42.
Dufwenberg, M., & Dufwenberg, M. A. (2018). Lies in disguise – A theoretical analysis of cheating. *Journal of Economic Theory, 175*, 248-264.
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*(3), 359-396.
Eling, M., & Wirfs, J. (2019). What are the actual costs of cyber risk events? *European Journal of Operational Research, 272*(3), 1109-1119.
Esho, N., & Sharpe, I. G. (1995). Long-run estimates of technological change and scale economies in a dynamic framework: Australian permanent building societies, 1974–1990. *Journal of Banking & Finance, 19*(7), 1135-1157.
Faccio, M., Marchica, M. T., & Mura, R. (2011). Large shareholder diversification and corporate risk-taking. *The Review of Financial Studies, 24*(11), 3601–3641.
Finch, G. (2016, May 20). Ecuador Bank Says It Lost $12 Million in Swift 2015 Cyber Hack. Bloomberg. Retrieved from https://www.bloomberg.com/news/articles/2016-05-20/ecuador-bank-says-it-lost-12-million-in-swift-2015-cyber-hack
Frischtak, C. (1992). Banking Automation and Productivity Change: The Brazilian Experience. *World Development., 20*(12), 1769-1784, .

FSB. (2017). *Financial Stability Implications from FinTech: Supervisory and Regulatory Issues that Merit Authorities' Attention.* Basel, Switzerland: Financial Stability Board. Retrieved from http://www.fsb.org/wp-content/uploads/R270617.pdf

Fu, X. M., Lin, Y. R., & Molyneux, P. (2014). Bank competition and financial stability in Asia Pacific. *Journal of Banking & Finance, 38*, 64-77.

Goetz, M. R. (2018). Competition and bank stability. *Journal of Financial Intermediation, 35* (Part A), 57-69.

Gopalakrishnan, R., & Mogato, M. (2016, May 19). Bangladesh Bank official's computer was hacked to carry out $81 million heist: diplomat. *Reuters: Business News*. Thomson Reuters. Retrieved from https://www.reuters.com/article/us-cyber-heist-philippines/bangladesh-bank-officials-computer-was-hacked-to-carry-out-81-million-heist-diplomat-idUSKCN0YA0CH

Gordon, L. A., & Loeb, M. P. (2002). Return on information security investments, myths vs realities. *Strategic Finance, 84*(5), 26-31.

Greer, S., Lodge, G., Mazzini, J., & Yanagawa, E. (2019). *Global Tech Spending Forecast: Banking Edition, 2019.* CELENT.

Gupta, S. D. (2018). Information technology and profitability: evidence from Indian banking sector. *International Journal of Emerging Markets, 13*(5), 1070-1087.

Haan, J. d., & Poghosyan, T. (2012). Size and earnings volatility of US bank holding companies. *Journal of Banking and Finance, 36*(11), 3008-3016.

Hancock, D., & Humphrey, D. B. (1997). Payment transactions, instruments, and systems: A survey. *Journal of Banking & Finance, 21*, 1573 -1624.

Hancock, D., Humphrey, D. B., & Wilcox, J. A. (1999). Cost reductions in electronic payments: The roles of consolidation, economies of scale, and technical change. *Journal of Banking & Finance, 23*, 391 - 421.

Härle, P., Havas, A., & Samandar, H. (2016, July). The future of bank risk management. *McKinsey Working Papers on Risk*. Retrieved from https://www.mckinsey.com/business-functions/risk/our-insights/the-future-of-bank-risk-management

He, Z., & Xiong, W. (2012). Dynamic Debt Runs. *The Review of Financial Studies, 25*(6), 1799-1843.

Holmstrom, B., & Tirole, J. (1997). Financial Intermediation, Loanable Funds, and the Real Sector. *The Quarterly Journal of Economics, 112*(3), 663-691.

Hurd, T. R. (2016). *Contagion! Systemic Risk in Financial Networks.* Springer International Publishing.

Imbierowicz, B., & Rauch, C. (2014). The relationship between liquidity risk and credit risk in banks. *Journal of Banking & Finance, 40*, 242–256.

Infante, L., & Piazza, M. (2014). Political connections and preferential lending at local level: Some evidence from the Italian credit market. *Journal of Corporate Finance, 29*, 246-262.

Jiménez, G., Ongena, S., Peydró, J.-L., & Saurina, J. (2012). Credit Supply and Monetary Policy: Identifying the Bank Balance-Sheet Channel with Loan Applications. *American Economic Review, 102*(5), 2301-2326.

Johnson, K. N. (2015). Managing Cyber Risk. *Georgia Law Review , 50*(2), 548-592.

Kaspersky. (2015, February 16). The greatest heist of the century: hackers stole $1 bln. Kaspersky Lab Daily. Retrieved from https://www.kaspersky.com/blog/billion-dollar-apt-carbanak/7519/

Kauffman, R. J., Liu, J., & Ma, D. (2015). Technology investment decision-making under uncertainty. *Information Technology and Management, 16*(2), 153–172.

Kim, H., Park, K., & Song, S. (2016). Banking Market Size Structure and Financial Stability: Evidence from Eight Asian Countries. *Emerging Markets Finance and Trade, 52*(4), 975-990.

Koette, M., & Poghosyan, T. (2009). The identification of technology regimes in banking: Implications for the market power-fragility nexus. *Journal of Banking & Finance, 33*(8), 1413-1422.

Koetter, M., & Noth, F. (2013). IT use, productivity, and market power in banking. *Journal of Financial Stability, 9*(4), 695–704.

Laeven, L., & Levine, R. (2009). Bank governance, regulation and risk taking. *Journal of Financial Economics, 93*(2), 259-275.

Laeven, L., Ratnovski, L., & Tong, H. (2016). Bank size, capital, and systemic risk: Some international evidence. *Journal of Banking & Finance, 69* (Supplement 1), S25–S34.

Lages, L. F. (2016). VCW-Value Creation Wheel: Innovation, technology, business, and society. *Journal of Business Research, 69*, 4849-4855.

Lente, H. v., Spitters, C., & Peine, A. (2013). Comparing technological hype cycles: Towards a theory. *Technological Forecasting and Social Change, 80*(8), 1615-1628.

Mee, P., & Schuermann, T. (2018, September 18). How a Cyber Attack Could Cause the Next Financial Crisis. *Harvard Business Review*.

Mehran, H., & Thakor, A. (2011). Bank Capital and Value in the Cross-Section. *The Review of Financial Studies, 24*(4), 1019-1067.

Murgia, M., & Megaw, N. (2019, February 25). Cyber attacks on financial services sector rise fivefold in 2018. *Financial Times*. Retrieved from https://www.ft.com/content/6a2d9d76-3692-11e9-bd3a-8b2a211d90d5

Ngonzi, T. T. (2016). *Theorizing ICT-based social innovation on development in the context of developing countries of Africa.* Captown: University of Cape Town.

Nikolopoulos, K. I., & Tsalas, A. I. (2017). Non-performing Loans: A Review of the Literature and the International Experience. In P. Monokroussos, & C. Gortsos, *Non-Performing Loans and Resolving Private Sector Insolvency. Palgrave Macmillan Studies in Banking and Financial Institutions.* Palgrave Macmillan.

Pawlowska, M. (2016). Does the size and market structure of the banking sector have an effect on the financial stability of the European Union? *The Journal of Economic Asymmetries, 14*(Part A), 112-127.

Roth, A. V., & Jackson-III, W. E. (1995). Strategic Determinants of Service Quality and Performance: Evidence from the Banking Industry. *Management Science, 41*(11), 1720-1733.

Schaeck, K., & Chiak, M. (2014). Competition, Efficiency, and Stability in Banking. *Financial Management, 43*(1), 215-241.

Shaddady, A., & Moore, T. (2019). Investigation of the effects of financial regulation and supervision on bank stability: The application of CAMELS-DEA to quantile regressions. *Journal of International Financial Markets, Institutions & Money, 58*, 96-116.

Shank, J. K. (1996). Analysing technology investments—from NPV to Strategic Cost Management (SCM). *Management Accounting Research, 7*(2), 185-197.

Tang, M.-J., & Zannetos, Z. S. (1992). Competition under Continuous Technological Change. *Managerial and Decision Economics, 13*, 135-148.

Tchamyou, V. S., Erreygers, G., & Cassimon, D. (2019). Inequality, ICT and financial access in Africa. *139*, 169-184.

Thomson Reuters. (2016, December 2). Russian central bank, private banks lose $31 mln in cyber attacks. Reuters: Technology News. Retrieved from https://www.reuters.com/article/us-russia-cenbank-cyberattack-idUSKBN13R1TO

Treanor, J. (2016, November 8). Tesco Bank cyber-thieves stole £2.5m from 9,000 people. The Guardian. Retrieved from https://www.theguardian.com/business/2016/nov/08/tesco-bank-cyber-thieves-25m

Uddin, M. H., & Ali, M. H. (2018). Cybersecurity Risk and Banking Stability - A thematic review. *Proceding (abstarct), 9th Annual Financial Market Liquidity Conference 15-16 November 2018* (p. 10). Budapest: Corvinus University.

Varotto, S., & Zhao, L. (2018). Systemic risk and bank size. *Journal of International Money and Finance, 82*, 45-70.

Vives, X. (2019). Competition and stability in modern banking: A post-crisis perspective. *International Journal of Industrial Organization*, In press.

Wagner, W. (2007). The liquidity of bank assets and banking stability. *Journal of Banking & Finance, 31*(1), 121–139.

Table 1: Sample distribution

No.	Country	Number of banks with annual reports available for 2008-17	Number of banks reporting cyber technology spending as on 2017	Number observations for cyber technology spending in 2008-17
1	Argentina	7	4	35
2	Australia	6	6	48
3	Bangladesh	18	14	101
4	Belgium	8	4	40
5	Brazil	17	6	51
6	Canada	4	4	31
7	Chile	9	3	28
8	China	9	8	76
9	Denmark	7	4	27
10	Egypt	9	7	39
11	Finland	4	3	22
12	France	12	8	61
13	Germany	6	5	44
14	Greece	5	5	50
15	India	16	8	51
16	Indonesia	10	5	44
17	Israel	5	4	21
18	Italy	8	6	60
19	Japan	6	3	30
20	Jordan	8	8	71
21	Malaysia	9	9	87
22	Mexico	7	3	27
23	Netherland	3	3	23
24	New Zealand	4	4	34
25	Norway	9	9	69
26	Oman	6	5	37
27	Pakistan	8	7	66
28	Poland	9	9	77
29	Qatar	4	4	28
30	Russia	8	4	31
31	Saudi Arabia	8	7	44
32	Singapore	3	3	22
33	South Africa	7	4	40
34	South Korea	5	4	25
35	Spain	8	4	37
36	Sweden	4	4	33
37	Switzerland	13	9	56
38	Thailand	6	4	24
39	Tunisia	7	5	26
40	Turkey	10	9	77
41	UAE	4	3	30
42	UK	6	6	50
43	USA	32	30	292
	Total	**354**	**264**	**2165**

We select the banks based on the availability of annual reports and relevant data in the databases.

Table 2: Variable descriptive statistics

Variables	Obs.	Mean	Std.Dev.	Minimum	Maximum	Skewness	Kurtosis
Z-score	3237	7.511	8.917	-1.719	48.795	2.301	9.354
Z-score (before taxes)	3047	6.438	7.113	-1.695	38.437	2.221	9.041
CyberTech-1	2164	3.042	2.179	-2.989	7.476	-0.318	2.983
CyberTech-1 squared	2164	14.139	13.47	0.009	55.889	1.220	3.861
CyberTech -2	2102	6.724	6.771	0.020	31.943	1.627	5.537
CyberTech-2 squared	2102	91.124	177.209	0.001	1020.36	3.274	14.793
Total asset	3341	9.843	1.922	5.749	14.484	0.337	2.609
Asset turnover	3307	0.048	0.036	0.007	0.214	2.595	10.777
Cost-to-income	3317	2.087	4.587	-17.612	25.931	1.270	16.214
Interest margin	3105	3.685	3.039	0.595	20.269	3.131	15.290
Tier-1 capital	2417	13.033	3.953	6.390	30.300	1.469	6.892
Equity-to-asset	3339	0.099	0.050	0.009	0.370	2.358	12.431
Non-performing loan	2270	3.920	4.915	0.133	30.738	3.001	14.129
Cybersecurity commitment	3540	0.592	0.184	0.176	0.919	-0.396	2.310
Corruption	3540	55.605	21.286	21.000	93.000	0.175	1.640
Financial freedom	3540	58.175	18.047	20.000	90.000	-0.294	2.219
Gross domestic product	3540	4.166	0.576	2.861	4.955	-0.676	2.380
Inflation	3540	4.113	5.593	-15.713	23.949	0.934	7.123

Z-score = (ROA + capital-asset ratio)/σROA. *CyberTech-1* is the natural log of the total cyber technology spending by sample bank. *CyberTech-1 squared* is the squared value of *CyberTech-1*. *CyberTech-2* is the cyber technology spending as a percent of non-interest operating costs. *CyberTech-2 squared* is the squared value of *CyberTech-2*. Z-score (before taxes) is estimated by using the return on asset based on operating income (instead of net income). *Total Asset* is the natural log of the total bank asset. *Asset turnover* is the total revenue divided by the total assets of the bank. The *cost-to-income* is the ratio of operating expense to operating income. *Interest margin* is the spread between the average lending and deposit interest rates of the bank. *Tier-1* is the ratio of a bank's core capital to the risk-weighted asset. *Equity-to-asset* is the total equity of the bank divided by its total asset. The *non-performing loan* is the non-performing loan as the percentage of the total loan of a bank. *Cybersecurity commitment* measures the commitment score of the country to cybersecurity as reported by International Telecommunication Union. *Corruption* is the corruption perception index of the country as reported by Transparency International. *Financial freedom* is the financial freedom index of a country provided by Heritage.org. *Gross domestic product* is the natural log of the real gross domestic product per capita of the country. *Inflation* is the annual rate of inflation of a country.

Table 3: Regression findings of banking stability and cyber technology spending measured as the natural log.

	Variables	OLS estimation		GMM estimation	
		Model 1 Linear test	Model 2 Non-linear	Model 3 Linear test	Model 4 Non-linear
Lag variable	*Z-score*$_{t-1}$			0.577***	0.564***
				(10.276)	(9.821)
Focused variables	*CyberTech-1*	0.166	0.799***	0.874*	3.144**
		(1.259)	(5.382)	(1.837)	(2.243)
	CyberTech-1 squared		-0.107***		-0.372**
			(-5.584)		(-2.047)
Bank-level controls	*Total asset*	0.467**	0.578***	0.285	0.420
		(2.349)	(2.684)	(0.603)	(0.708)
	Asset turnover	-18.424	-15.286	-10.500	7.384
		(-0.871)	(-0.729)	(-0.305)	(0.190)
	Cost to income	-0.113**	-0.114**	0.088	0.114
		(-2.225)	(-2.305)	(0.933)	(1.183)
	Interest margin	0.357	0.332	0.286	-0.104
		(1.268)	(1.202)	(0.662)	(-0.198)
	Tier-1 capital	0.145	0.144	0.020	0.024
		(1.371)	(1.342)	(0.174)	(0.195)
	Equity-to-asset	28.729***	27.926***	38.075	33.397
		(3.432)	(3.358)	(1.570)	(1.362)
	Non-performing loan	-0.529***	-0.529***	-0.233*	-0.286**
		(-11.460)	(-11.296)	(-1.894)	(-2.101)
Country-level controls	*Cybersecurity commitment*	1.760	1.853	-1.033	-2.338
		(0.693)	(0.717)	(-0.276)	(-0.588)
	Corruption	0.052	0.058	-0.006	-0.007
		(1.454)	(1.654)	(-0.082)	(-0.001)
	Financial freedom	-0.072**	-0.076**	0.106	0.116
		(-2.139)	(-2.423)	(1.468)	(1.500)
	Gross domestic product	-4.664***	-4.641***	-5.140**	-5.955**
		(-4.990)	(-4.802)	(-2.175)	(-2.233)
	Inflation	-0.298***	-0.298***	-0.015	-0.051
		(-3.215)	(-3.265)	(-0.111)	(-0.354)
Fixed effect	*Country and Year*	-0.000***	-0.000***	*See note*	*See note*
		(-3.665)	(-4.539)		
	Constant	22.211***	20.463***	10.407	11.665
		(3.310)	(2.958)	(1.130)	(1.149)
	Observations	1356	1356	1256	1256
	F-Value (OLS)/Wald χ^2 (GMM)	28.210	27.340	386.090	350.520
	R-squared	0.185	0.189		

We estimate $Zscore_{it} = \alpha_i + \beta_i CyberTech1_{it} + \sum_{i=1}^{n} \gamma Control_{it} + \varepsilon_{it}$ using OLS and dynamic panel of system GMM. We include $Zscore_{it-1}$ as a lag variable in the GMM model. Z-*score* is banking stability proxy calculated as (ROA + capital-asset ratio)/σROA; where ROA equals the ratio of net income to the total asset. *CyberTech-1* is natural log of the total cyber technology related expense incurred by the bank. *Controls* are vectors of control variables defined in Appendix-1. The country and year interaction variable is used in OLS estimation based on literature (Beck *et al*, 2013), but not applied in system GMM as supporting literature is unavailable. The values within parenthesis are robust *t-stats* adjusted for heteroscedasticity. Asterisks ***, **, and * denote significance at the less than 1%, 5%, and 10% levels.

Table 4: Regression findings of banking stability and cyber technology spending measured as the percentage of non-interest expense.

Variables		OLS estimation		GMM estimation	
		Model 1 Linear test	Model 2 Non-Linear	Model 3 Linear test	Model 4 Non-linear test
Lag variable	*Z-score$_{t-1}$*			-0.150*** [-4.874]	-0.151*** (-3.420)
Focused variables	*CyberTech-2*	0.060** (2.398)	0.171** (2.720)	0.170* (1.940)	0.557** (2.114)
	CyberTech-2 squared		-0.005** (-2.240)		-0.012* (-1.788)
Bank-level controls	*Total asset*	0.647*** (3.442)	0.639*** (3.500)	1.346 (0.915)	1.183 (0.885)
	Asset turnover	-18.021 (-0.856)	-16.283 (-0.770)	71.358 (1.437)	78.728* (1.940)
	Cost to income	-0.111** (-2.183)	-0.111* (-2.170)	-0.008 (-0.199)	-0.009 (-0.666)
	Interest margin	0.382 (1.345)	0.364 (1.280)	1.156** (2.275)	1.169** (2.539)
	Tier1 capital	0.144 (1.393)	0.148 (1.400)	-0.186 (-1.189)	-0.198 (-1.552)
	Equity-to-asset	28.845*** (3.495)	27.508** (3.180)	7.766 (0.360)	8.386 (0.473)
	Non-performing loan	-0.526*** (-11.106)	-0.524*** (-11.180)	-0.188 (-1.454)	-0.199* (-1.657)
Country-level controls	*Cybersecurity commitment*	1.760 (0.691)	1.654 (0.660)	-16.687*** (-3.959)	-17.197** (-2.226)
	Corruption	0.050 (1.381)	0.512 (1.410)	0.099 (1.444)	0.096 (1.260)
	Financial freedom	-0.071** (-2.046)	-0.074* (-2.160)	-0.025 (-0.365)	-0.022 (-0.353)
	Gross domestic product	-4.644*** (-5.051)	-4.707*** (-5.070)	37.507*** (3.212)	36.991** (2.481)
	Inflation	-0.296*** (-3.192)	-0.297*** (-3.230)	-0.128** (-2.342)	-0.135* (-1.729)
Fixed effect	*Country and Year*	-0.000*** (-3.446)	-0.000*** (-3.390)	*See note*	*See note*
	Constant	20.287*** (2.744)	20.420** (2.770)	-165.218*** (-3.799)	-162.854** (-2.436)
	Observations	1356	1356	1041	1041
	F-Value (OLS)/Wald χ^2 (GMM)	27.940***	26.390***	74.81***	71.49***
	R-squared	0.189	0.187		

We estimate $Zscore_{it} = \alpha_i + \beta_i CyberTech2_{it} + \sum_{i=1}^{n} \Upsilon Control_{it} + \varepsilon_{it}$ using OLS and dynamic panel of system GMM. We include $Zscore_{it-1}$ as a lag variable in the GMM model. Z-*score* is banking stability proxy calculated as (ROA + capital-asset ratio)/σROA; where ROA equals the ratio of net income to the total asset. *CyberTech-2* is the cyber technology related expense as the percentage of non-interest expense incurred by the bank. *Controls* are vectors of control variables defined in Appendix-1. The country and year interaction variable is used in OLS estimation based on literature (Beck *et al*, 2013), but not applied in system GMM as supporting literature is unavailable. The values within parenthesis are robust *t-stats* adjusted for heteroscedasticity. Asterisks ***, **, and * denote significance at the less than 1%, 5%, and 10% levels.

Table 5: Fixed effect (FE) panel regression findings of banking stability and cyber technology spending.

Variables		FE panel regressions for the natural log of cyber technology spending.		FE panel regressions for the cyber technology spending as the percentage of non-interest expense.	
		Model 1 Linear	Model 2 Non-linear	Model 3 Linear	Model 4 Non-linear
Focused variables	*CyberTech-1*	-0.502 (-0.39)	0.629*** (3.68)		
	CyberTech-1 squared		-0.113*** (-5.19)		
	CyberTech-2			0.007 (0.30)	0.136*** (2.63)
	CuberTech-2 squared				-0.005*** (-2.91)
Bank-level controls	*Total asset*	0.617*** (3.07)	0.734*** (3.48)	0.579*** (3.30)	0.575*** (3.36)
	Asset turnover	-20.556 (-0.78)	-17.935 (-0.68)	-21.869 (-0.81)	-20.096 (-0.75)
	Cost to income	-0.135*** (-2.61)	-0.136*** (-2.67)	-0.135*** (-2.62)	-0.135** (-2.62)
	Interest margin	0.514 (1.63)	0.493 (1.57)	0.519 (1.63)	0.501 (1.57)
	Tier1 capital	-0.013 (-0.12)	-0.189 (-0.18)	-0.006 (-0.06)	-0.000 (-0.00)
	Equity-to-asset	20.493*** (2.99)	18.979*** (2.92)	20.37*** (2.94)	19.118*** (2.67)
	Non-performing loan	-0.561*** (-12.89)	-0.559*** (-12.80)	-0.562*** (-12.43)	-0.560*** (-12.58)
Country-level controls	*Cybersecurity commitment*	-1.170 (-0.69)	-1.316 (-0.79)	-1.20 (-0.67)	-1.367 (-0.79)
	Corruption	0.059* (1.98)	0.067** (2.42)	0.058* (1.95)	0.059* (1.97)
	Financial freedom	-0.080* (1.99)	-0.843** (-2.26)	-0.80* (-1.98)	-0.084** (-2.07)
	Gross domestic product	-4.514*** (-3.95)	-4.529*** (-3.90)	-4.482*** (-3.97)	-4.502*** (-3.95)
	Inflation	-0.381*** (3.32)	-0.370*** (-3.06)	-0.375*** (-3.34)	-0.371*** (-3.29)
	Constant	24.241*** (3.32)	22.544*** (2.99)	24.359*** (3.09)	24.267*** (3.10)
	Observations	1356	1356	1356	1356
	F-Value	22.70	21.72***	22.70***	21.22***
	R-squared	0.181	0.186	0.182	0.182

We estimate the base model $Zscore_{it} = \alpha_i + \beta_i CyberTech_{it} + \sum_{i=1}^{n} \gamma Control_{it} + \varepsilon_{it}$ as a fixed effect panel regression. We apply Z-*score* as the proxy of banking stability variable, which is calculated as (ROA + capital-asset ratio)/σROA. In this estimation, ROA equals the ratio of net income to total asset. We test two proxies for cyber technology spending: *CyberTech-1* is the natural log of total cyber technology related expense and *CyberTech-2* is the cyber technology related expense as the percentage of non-interest expense. *Controls* are vectors of bank- and country-level variables defined in Apendix-1. The values in parenthesis are robust *t-stats* adjusted for heteroscedasticity, and asterisks ***, **, and * denote significance at the less than 1%, 5%, and 10% levels.

Table 6: Bank stability and cyber technology spending by bank size

Variables		Small banks		Large banks	
		Model 1 Linear	Model 2 Non-linear	Model 3 Linear	Model 4 Non-linear
Focused variables	*CyberTech-1*	0.055	0.199	0.174	1.118*
		(0.181)	(0.794)	(1.225)	(2.063)
	CyberTech-1 squared		-0.124*		-0.128*
			(-2.206)		(-2.041)
Bank-specific variables	*Total asset*	1.875***	1.965***	-0.016	0.235
		(4.984)	(4.781)	(-0.081)	(1.000)
	Asset turnover	2.337	8.417	-53.551	-46.870
		(0.042)	(0.154)	(-1.643)	(-1.469)
	Cost to income	-0.075	-0.070	-0.125**	-0.126**
		(-1.669)	(-1.511)	(-2.528)	(-2.603)
	Interest margin	0.172	0.155	0.881*	0.854*
		(0.304)	(0.277)	(2.008)	(1.986)
	Tier 1 capital	0.090	0.098	0.262**	0.245**
		(0.497)	(0.536)	(2.750)	(2.564)
	Equity to asset	24.588*	22.034	22.650**	23.646**
		(1.868)	(1.664)	(2.485)	(2.604)
	Non-performing loan	-0.375***	-0.367***	-0.538***	-0.542***
		(-3.643)	(-3.573)	(-10.991)	(-10.965)
Country-specific variables	*Cybersecurity commitment*	-3.164	-2.467	3.025	3.063
		(-0.647)	(-0.498)	(1.084)	(1.091)
	Corruption	0.142***	0.158***	0.034	0.032
		(5.305)	(5.512)	(0.768)	(0.741)
	Financial freedom	-0.083	-0.088	-0.053	-0.052
		(-1.637)	(-1.721)	(-1.601)	(-1.564)
	Gross domestic product	-2.810*	-2.931**	-5.863***	-5.729**
		(-2.152)	(-2.335)	(-3.264)	(-3.102)
	Inflation	-0.079	-0.088	-0.403***	-0.405***
		(-0.854)	(-0.946)	(-3.423)	(-3.502)
Fixed effects	*Country and Year*	-0.000	-0.000	-0.000**	-0.000**
		(-1.366)	(-1.572)	(-2.637)	(-2.494)
	Constant	0.164	-0.330	31.711***	26.745**
		(0.022)	(-0.040)	(3.527)	(2.481)
	Observations	393	393	963	963
	F-value	8.380	7.980	14.850	14.830
	R-square	0.149	0.153	0.208	0.210

We estimate $Bank\ stability_{it} = \alpha + \beta CyberTech1_{it} + \gamma Controls_{it} + \varepsilon_{it}$. We classify the sample into two size-groups based on the median value of the log of total assets. The small banks are those below the median value while the large banks are those above the median. we apply *CyberTech1* as focused explanatory variable which is the natural log of total cyber tech spending mentioned as absolute value, and *Z-score* as the proxy of bank stability. Values in parenthesis are robust *t-stats* adjusted for heteroscedasticity in the data. and asterisks ***, **, and * denote significance at the less than 1%, 5%, and 10% levels.

Table 7: Bank stability and cyber technology spending across different levels of cyber technology advancement in the country

Variables		Initiating level		Maturing level		Leading level	
		Model 1 Linear	Model 2 Non-linear	Model 3 Linear	Model 4 Non-linear	Model 5 Linear	Model 6 Non-linear
Focused variables	*CyberTech-1*	0.977*	0.254	0.647***	1.697**	-0.843**	-0.112
		(1.903)	(0.380)	(3.707)	(2.532)	(-2.446)	(-0.756)
	CyberTech-1 square		0.120		-0.151*		-0.169***
			(1.041)		(-2.007)		(-5.395)
Bank-level variables	*Total asset*	0.883	0.805	-0.420	-0.284	1.361***	1.807***
		(1.827)	(1.575)	(-1.305)	(-0.834)	(3.792)	(5.072)
	Asset turnover	32.587	25.390	-39.219	-39.590	20.590	42.582
		(0.330)	(0.246)	(-1.395)	(-1.430)	(0.551)	(1.104)
	Cost to income	-0.163*	-0.164*	-0.063	-0.071	-0.090*	-0.085*
		(-2.251)	(-2.092)	(-1.130)	(-1.220)	(-2.009)	(-1.958)
	Interest margin	-0.035	0.044	0.557*	0.575*	-0.286	-0.450
		(-0.035)	(0.040)	(1.937)	(1.997)	(-0.808)	(-1.340)
	Tier 1 capital	-0.016	-0.013	0.612***	0.598***	0.210	0.217
		(-0.113)	(-0.087)	(5.479)	(5.466)	(1.506)	(1.682)
	Equity to asset	37.575**	38.215**	5.313	3.311	-3.683	-3.575
		(2.997)	(2.950)	(0.517)	(0.343)	(-0.209)	(-0.214)
	Non-performing loan	-0.432***	-0.435***	-0.528***	-0.54***	-1.073***	-1.047***
		(-3.849)	(-3.825)	(-10.923)	(-12.69)	(-5.610)	(-5.495)
Country-level variables	*Cybersecurity Commit*	-10.00***	-9.902***	-16.675*	-13.733	45.142***	44.286***
		(-3.537)	(-3.742)	(-2.144)	(-1.833)	(4.533)	(4.338)
	Corruption	0.152***	0.140**	-0.030	-0.037	0.058	0.049
		(3.494)	(3.204)	(-1.259)	(-1.447)	(0.922)	(0.798)
	Financial freedom	-0.149***	-0.140***	-0.024	-0.029	-0.046	-0.061**
		(-3.754)	(-3.732)	(-0.602)	(-0.789)	(-1.604)	(-2.523)
	Gross domestic product	-6.384***	-5.982***	-5.731***	-5.351**	-6.648**	-4.923*
		(-5.323)	(-5.515)	(-3.462)	(-3.151)	(-2.609)	(-2.056)
	Inflation	-0.349**	-0.344**	-0.348**	-0.348**	-0.132	-0.128
		(-2.353)	(-2.335)	(-2.298)	(-2.303)	(-1.224)	(-1.165)
Fixed effects	*Country and Year*	0.000	0.000	-0.000	-0.000	-0.000***	-0.000***
		(1.612)	(1.585)	(-1.474)	(-1.292)	(-3.773)	(-4.808)
	Constant	23.703**	23.412**	43.157***	37.93***	-7.520	-17.199
		(2.538)	(2.528)	(4.452)	(3.780)	(-0.541)	(-1.253)
	Observations	368	368	372	372	616	616
	F-value	11.460	10.790	7.970	7.890	13.640	14.810
	R-square	0.283	0.285	0.305	0.310	0.189	0.201

We estimate $Bank\ stability_{it} = \alpha + \beta CyberTech1_{it} + \gamma Controls_{it} + \varepsilon_{it}$. We sort the sample banks into three classes based on the level of cyber technology advancement in the country as determined by International Telecommunication Union (ITU). The initiating-level countries are those with a score below the 33th percentile, the maturing level countries are those with a score between the 33th and 67th percentiles, and the leading countries are those with a score above the 67th percentile. We apply *CyberTech1* as focused explanatory variable which is the natural log of total cyber tech spending mentioned as absolute value, and *Z-score* as the proxy of bank stability. Values in parenthesis are robust *t-stats* adjusted for heteroscedasticity in the data., and asterisks ***, **, and * denote significance at the less than 1%, 5%, and 10% levels.

Table 8: Bank stability and cyber technology spending in pre-fintech and fintech era

Variables		Pre-fintech era		Fintech era	
		Linear	Non-linear	Linear	Non-linear
Focused variables	*CyberTech-1*	0.054	0.306	0.086	0.782***
		(0.155)	(1.280)	(0.788)	(8.362)
	CyberTech-1 square		-0.040		-0.119***
			(-2.601)		(-6.462)
Bank-specific variables	*Total asset*	-0.235	-0.199	0.638**	0.766**
		(-1.484)	(-1.281)	(3.097)	(3.430)
	Asset turnover	47.354	47.490	-20.987	-17.086
		(0.888)	(0.870)	(-0.933)	(-0.759)
	Cost to income	0.019	0.016	-0.151**	-0.150**
		(0.762)	(0.680)	(-2.907)	(-2.966)
	Interest margin	-0.403	-0.402	0.538	0.506
		(-0.819)	(-0.789)	(1.892)	(1.801)
	Tier 1 capital	-0.247**	-0.244***	0.077	0.074
		(-44.802)	(-220.143)	(0.661)	(0.630)
	Equity to asset	13.867**	13.832**	31.025**	29.795**
		(50.709)	(44.241)	(3.179)	(3.023)
	Non-performing loan	-0.658	-0.651	-0.529***	-0.530***
		(-3.324)	(-3.254)	(-9.155)	(-9.148)
Country-specific variables	*Cybersecurity*	-2.797	-2.881	0.997	1.134
		(-1.153)	(-1.193)	(0.333)	(0.374)
	Corruption	0.027	0.029	0.075*	0.082*
		(0.418)	(0.467)	(1.934)	(2.156)
	Financial freedom	-0.081	-0.082	-0.075	-0.080*
		(-1.370)	(-1.386)	(-1.680)	(-1.933)
	Gross domestic product	-3.031*	-3.013*	-5.299***	-5.276***
		(-11.319)	(-7.991)	(-5.453)	(-5.171)
	Inflation	-0.146	-0.144	-0.365**	-0.367**
		(-3.249)	(-2.930)	(-3.353)	(-3.398)
Fixed effects	*Country and Year*	0.000	0.000	-0.000***	-0.000***
		(0.723)	(0.727)	(-3.033)	(-4.047)
	Constant	28.002***	27.197***	23.689**	21.859**
		(66.366)	(127.039)	(2.942)	(2.650)
	Observations	200	200	1156	1156
	F-value	4.530**	4.320**	19.040***	19.350***
	R-square	0.173	0.172	0.199	0.203

We estimate $Bank\ stability_{it} = \alpha + \beta CyberTech1_{it} + \gamma Controls_{it} + \varepsilon_{it}$. We classify the sample into two sub-set: pre-fintech period (2008-9) and post-crisis fintech period (2010-2017). We apply *CyberTech-1* as focused explanatory variable which is the natural log of total cyber tech spending mentioned as absolute value, and *Z-score* as the proxy of bank stability. Values in parenthesis are robust *t-stats* and asterisks ***, **, and * denote significance at the less than 1%, 5%, and 10% levels.

Table 9: Robustness tests with alternative measures of dependent and independent variables

Focused Variables	**Panel A: Tests with Z-score (before taxes) as the dependent variable** $Bank\ stability_{it} = \alpha_i + \beta_1 CyberTech_{it} + \sum_{i=1}^{n} \gamma Control_{it} + \varepsilon_{it}$ Appendix-1 provides details of the test variables. In the nonlinear estimations, we apply *CyberTech squared* as an additional variable.				**Panel B: Tests with a different measure of focused explanatory variable** $Bank\ stability_{it} = \alpha + \beta_1 CyberTech_{High} + \beta_2 CyberTech_{Low} + \sum_{i=1}^{n} \gamma Control_{it} + +\varepsilon_{it},$ See notes at the bottom of this table:	
	Linear	Non-linear	Linear	Non-linear	Z-score	Before-tax Z-score
CyberTech-1	-0.059	0.456***				
	(-0.822)	(2.615)				
CyberTech-1 squared		-0.087***				
		(-3.561)				
CyberTech-2			0.036**	0.129**		
			(2.122)	(2.299)		
CuberTech-2 squared				-0.004*		
				(-1.784)		
$CyberTech_{High}$					-1.396***	-1.480***
					(-3.360)	(-3.870)
$CyberTech_{Low}$					0.296	0.708
					(0.46)	(1.14)
Controls	Yes	Yes	Yes	Yes	Yes	Yes
Country and year effect	-0.000***	-0.000***	-0.000***	-0.000***	-0.000	-0.000*
	(-3.281)	(-4.043)	(-2.954)	(-3.360)	(-1.46)	(-1.69)
Constant	10.601**	9.060*	10.516**	20.204***	17.510***	8.270***
	(2.063)	(1.668)	(2.002)	(2.735)	(5.530)	(2.630)
Observations	1309	1309	1356	1356	1827	1738
F-value	33.180***	32.060***	32.450***	26.240***	16.53***	17.410***
R-squared	0.194	0.198	0.200	0.187	0.178	0.200

In Panel B, $CyberTech_{High}$ = 1 if the natural log of total cyber technology spending is greater than the 75th percentile, otherwise 0. $CyberTech_{Low}$ = 1 if the natural log of total cyber technology spending is less than the 25th percentile, otherwise 0. The banks with cyber technology spending between the 25th and 75th percentiles are considered as the base group. Other variables are the same as those in the earlier tables. For both panels, we checked fixed effect models, but significance levels do not change. The values in parenthesis are robust *t-stats* with standard errors clustered by country and year. We cannot report control variable results here due to space limitation. Asterisks ***, **, and * denote significance at the less than one, five, and ten percent levels in both panels.

Table 10: Findings by region and country

Country and region	Linear test	Non-linear test	
	CyberTech	*CyberTech*	*CyberTech Squared*
USA	0.052	0.508*	-0.018**
Canada	-0.004	-2.398	0.144
North America	**-0.163****	**0.215**	**-0.016****
UK	-0.081**	0.082	-0.005
Germany	-1.103***	-4.947***	0.236***
France	0.129	0.005	0.006
Belgium	-0.494***	-0.902	0.020
Italy	-1.229***	-2.448***	0.229
Greece	-0.005	0.094	-0.002
Spain	0.529**	1.915	-0.085
Poland	0.054	1.205***	-0.030***
Switzerland	-0.040	1.606*	-0.093
Netherland	0.139	-0.962	0.092*
Finland	-0.111	-1.883***	0.087***
Denmark	-0.191**	-0.722***	0.018***
Norway	-0.047	0.291***	-0.012***
Sweden	-0.521***	-1.935*	0.140
Europe	**0.262**	**0.519****	**-0.043***

Country and region	Linear test	Non-linear test	
	CyberTech	*CyberTech*	*CyberTech Squared*
Bangladesh	-0.032	-0.597**	0.0183**
China	0.144	0.891	-0.036
India	-0.792	3.308	-0.562
Pakistan	0.630**	2.937**	-0.387**
Thailand	-0.339	-2.329***	0.198**
Indonesia	-0.324**	-0.915	0.021
Malaysia	-0.030	0.127	-0.004
Singapore	-1.588***	-7.327*	0.246
Japan	-0.095	0.529	-0.017
Korea	-1.420**	1.258	-0.256*
Asia	**-0.085**	**0.080**	**-0.008**
Australia	0.126*	0.192	-0.0024
New Zealand	-0.295	-17.650	4.068
Asia Pacific	**-0.010**	**0.672**	**-0.025**
Argentina	0.029	-3.387**	0.6227**
Brazil	-0.327***	-0.465**	0.005
Chile	0.056	0.166	-0.004
Mexico	0.100	8.628***	-1.269***
Latin America	**0.016**	**0.436**	**-0.014**

Country and region	Linear test	Non-linear test	
	CyberTech	*CyberTech*	*CyberTech Squared*
Egypt	-0.040	0.246	-0.013
Israel	1.164**	0.988	0.005
Jordan	0.374	1.446*	-0.047
Oman	-0.368***	-1.351***	0.028**
Qatar	-0.178	1.769	-0.097
Saudi	0.240	-0.401	0.0456
Tunisia	0.073	0.735*	-0.026*
Turkey	-0.276***	-1.127**	0.053**
UAE	1.289	6.150*	-1.279*
MENA	**0.133**	**0.768****	**-0.023****
Russia	-0.013	0.056	-0.002
South Africa	-0.552	2.403	-0.473*
Others	**1.787**	**1.799****	**-1.999****

The base model is:

$Bank\ stability_{it} = \alpha + \beta CyberTech_{it} + \gamma Controls_{it} + \varepsilon_{it}$. We test both *CyberTech-1* and *CyberTech-2* as different measures of cyber technology spending. We add *CyberTech-1 squared* and *CyberTech-2 squared* as the additional variables. As results are consistent for both estimations of cyber technology spending, we report here only those based on *CyberTech-2* due to space limitation. Asterisks ***, **, and * denote significance at the less than one, five, and ten percent levels.

Appendix 1: Variables description

Dependent variables			
Variables	**Descriptions**	**Source**	**References**
Z-score	*Z-score* = (ROA + capital-asset ratio)/σROA, which measures the financial stability of banks.	Authors' calculation	Demirgüç-Kunt, Detragiache, & Tressel (2008); Laeven & Levine, (2009); Čihák & Hesse (2010); Beck, Demirguc-Kunt, & Merrouche (2013); Chiaramonte, Liu, Poli, & Zhou (2016);
Z-score (before taxes)	*Z-score (before taxes)* is estimated by using the ROA based on operating income before taxes. Prior researchers measured risk proxies (σROA) based on the operating income instead of the net income after taxes.	Authors' calculation	Boubakri, Cosset, & Saffar, (2013); Faccio, Marchica, & Mura, (2011)
Focused independent variables			
CyberTech-1	*CyberTech-1* is the natural log of CyberTech spending in the bank, the total cost covers the data processing, third-party security providing services, computer and software development, IT personnel training in the income statement and current year amortization of software and computer in separate notes to the financial statement.	Manual collection form annual report	Our study
CyberTech-1 squared	*CyberTech-1 squared* refers to the squared value of *CyberTech-1*	Authors' calculation	Our study
CyberTech-2	*CyberTech-2* is the percentage of total non-interest operating expenses.	Manual collection form annual report	Our study
CyberTech-2 squared	*CyberTech-2 squared* refers to the squared value of *CyberTech-2*	Authors' calculation	Our study
$CyberTech_{High}$	$CyberTech_{High}$ = 1 if the natural log of total cyber technology spending is greater than the 75th percentile, otherwise 0.	Authors' calculation	Our study
$CyberTech_{Low}$	$CyberTech_{Low}$ = 1 if the natural log of total cyber technology spending is less than the 25th percentile, otherwise 0	Authors' calculation	Our study
Bank-level control variables			
Total asset	*Total asset* is the average of the beginning balance and ending balance in the balance sheet	Bloomberg	Haan & Poghosyan (2012)
Asset turnover	*Asset turnover* is the total revenue divided by total asset	Authors' calculation	Wagner (2007)

Cost to income	The *cost-to-income* is the ratio of operating expense to operating income.	Bloomberg	Schaeck & Chiak (2014)
Interest margin	*Net interest margin* in percentage is a performance metric that examines how successful a firm's investment decisions are compared to its debt situations. A negative value denotes that the firm did not make an optimal decision, because interest expenses were greater than the amount of returns generated by investments.	Bloomberg	Chaudron (2018)
Tier-1 capital	*Tier-1* is the ratio of a bank's core capital to the risk-weighted asset. %. In Europe it is referred to as the BIS ratio, the European Solvency ratio, or the Cooke ratio as the Cooke committee established it	Bloomberg	Anginer, Demirgüc-Kunt, & Mare (2018b)
Equity to asset	*Equity-to-asset* is the total equity of the bank divided by its total asset. Average Total Common Equity is the average of the beginning balance and ending balance and Total asset is the average of the beginning balance and ending balance in the balance sheet	Authors' calculation	Anginer, Demirgüc-Kunt, & Mare (2018b)
Non-performing loan	The *non-performing loan* is the non-performing loan as the percentage of the total loan of a bank. Total loan is the sum of short-and long-term loans	Authors' calculation	Nikolopoulos & Tsalas, (2017) .Review paper.
Country-level control variables			
Cybersecurity	*Cybersecurity commitment* measures the commitment score of the country to cybersecurity protection.	International Telecommunication Union	Our study
Corruption	*The Corruption* Perceptions Index measures the perceived levels of public sector corruption in countries worldwide, the score ranging from 0 (highly corrupt) to 100 (very clean).	Transparency International	Infante & Piazza (2014)
Financial freedom	This is the financial freedom index of a country provided by Heritage.org. We take this variable because study finds that higher financial freedom in the economy promotes the level of banking efficiency.	The Heritage Foundation	Chortareas, Girardone, & Ventouri (2013)
Gross domestic product	*Gross domestic product* is the natural log of the real gross domestic product (GDP) per capita of the country denominated in USD. Evidence shows that GDP influences banking performance through monetary policy shocks	World Bank	Jiménez, Ongena, Peydró, & Saurina 2012)
Inflation	*Inflation* is consumer price index of a country.	World Bank	Boyd, Levine, & Smith (2001)
Fixed effect control			
*Country * year*	*Country*time* is an interaction between country and year to capture the heterogeneity of country and year fixed effect.	Authors' calculation	Beck, Demirguc-Kunt, & Merrouche (2013)

Figure 1: Pattern of relationship between banking stability and cyber technology spending