JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125 VOL 08, ISSUE 05, 2021

A Case Study on How U.S. Banks Respond to Cyber Insurance and How It Affects Their Operational Cyber Risk Mitigation

Dr. Munaga Ramakrishna Mohan Rao, MBA, Ph.D, LMISTE, PGDCA IC-38
Professor, Siddhartha Institute of Technology and Sciences, Hyderabad

Abstract- When an organization's IT system crashes, it may result in devastating consequences for the bottom line, including disruption, damage, or even destruction of operations. The cyber world is intricate, fragile, and risky. Therefore, banks as early adopters of IT have had to deal with the ever-evolving cyber risk and its escalating threats, vulnerabilities, and consequences. Financial institutions have employed a wide range of cyber risk mitigation strategies to counteract non-systemic cyber risk, with cyber insurance and the enhancement of operational cyber risk mitigation programmes and activities seen as particularly effective means of closing the gap between cyber risk and cybersecurity. However, there is currently few empirical data supporting this idea, therefore the literature in its favour remains mostly theoretical. This case study helps to close that knowledge gap by collecting and analysing information on how cyber risk insurance is actually purchased and how operational cyber risk mitigation strategies and activities may be enhanced. The authors used a mixed-method approach and found that while most of the cyber insurance variables in this study had an unpredictable or negative impact on operational cyber risk mitigation programmes and activities, three of the independent cyber insurance variables of how long a bank has been purchasing cyber privacy insurance, whether or not a bank has cyber risk, cyber network security, or cyber privacy insurance coverage, and whether or not a bank has a data breach policy were significantly associated with operational cyber risk mitigation programmes and activities. When it comes to information technology and cyber security, does the bank source its own supplies, or do its contractors make such purchases? Does the financial institution use outside vendors? had positive qualitative and quantitative results, improving the dependent operational cyber risk mitigation functional factors in major banks in New Jersey. These results will be useful for academic scholars and banking sector personnel alike.

Keywords— Cyber risk, Mitigation, Risk, Banking, Case Study, Response.

I. INTRODUCTION

Financial institutions have increased cyber risk, vulnerabilities, and consequences [1] due to their early adoption of new technologies. Banks are the lifeblood of national economies and a frequent target of cybercriminals, terrorists, and nation governments driven by geopolitical concerns [2]. Senior decision-makers in the financial sector may choose from a broad range of cyber

ISSN- 2394-5125 VOL 08, ISSUE 05, 2021

mitigation strategies designed to assist them reduce or eliminate non-systemic cyber risk, or at least lessen the impact of any cyber-incident that does occur [3]. Although the cyber landscape is always evolving, banks have had a hard time determining how to best manage their cyber risk with the limited resources at their disposal [4].

In 2006, Hahn and Layne-Farrar [5] proposed the idea that cyber insurance and enhanced operational cyber risk mitigation programmes and activities could work together to mitigate cyber risk, with the combined efforts being more effective at bridging the gap between cyber risk and cybersecurity and making better use of limited cybersecurity resources. Financial institutions may be able to decrease the gap between their cyber risk and their cybersecurity countermeasures down to a level that is compatible with their cyber risk tolerance and the resources they have to mitigate cyber risk by combining these two tactics [4]. While there is some evidence from the academic literature that including cyber insurance in operational cyber risk mitigation programmes and activities can help, the current state of this knowledge is not sufficient for practitioners in the banking industry to use when making strategic cybersecurity decisions. A missing link between academia and practise, according to Hubbard and Seiersen [6], is the availability of empirical data providing the level of detail necessary for top-level decision making. This case study of large New Jersey banks was conducted in response to a paucity of knowledge in this area, with the goal of educating bank decision-makers and adding to the conversation about the best ways to reduce cybersecurity risks at financial institutions [6].

II. RELATEDWORKS

It has been hypothesised that banks might lessen their exposure to non-systemic cyber risk by combining two approaches: cyber insurance and enhanced operational cyber risk mitigation programmes and activities. For the purposes of this paper, we will refer to cyber insurance as a financial instrument purchased by businesses to transfer economic risk associated with cyber losses due to disruption, damage, or destruction of IT systems as a result of activities like data theft or loss, system downtime, network intrusion, or cybersecurity breaches [7]. Programs and actions that assist banks manage cybersecurity risk via data organisation, risk management decision facilitation, vulnerability reduction, and best practise refining are referred to as operational cyber risk mitigation [3, 4].

Both improving operational cyber risk mitigation programmes and activities and investing in cyber risk insurance have been shown to be more effective together than individually [4]. Why? Because when used together, they help reduce cyber risk and increase security while making better use of limited resources. Since 2006, researchers have recognised that cyber insurance is associated with better operational cyber risk mitigation programmes and activities. However, the reasons for this correlation have shifted over time, from the rational management decision-making of Hahn and Layne-Farrar [5] to the fear of regulation posed by Dandapani [8] to the influence of the board of directors [4]. Use of limited cyber risk mitigation resources effectively may help a bank meet its risk tolerance threshold [4]. Purchasing cyber risk insurance and

ISSN- 2394-5125 VOL 08, ISSUE 05, 2021

enhancing operational cyber risk mitigation plans and actions are both effective ways to achieve this goal.

Investment in cyber risk insurance has been shown to correlate with higher investment in operational cyber risk mitigation programmes and activities, however this is not yet proven in the literature. Board of directors and upper management decision making is slowed by a lack of empirical evidence since there is no bridge between academia and practise [6]. Senior bank managers and board members will benefit from this study because they will have more information with which to make educated choices and maximise the limited cybersecurity mitigation resources at their disposal. Since the financial sector has long been at the forefront of cyber threats and cybersecurity, there has been a commensurate increase in spending on cybersecurity countermeasures and a greater focus on reducing and managing cyber risk [9]. This study utilises information from a selection of major New Jersey banks to check whether the phenomenon under study may be seen and tested.

III. PROPOSED SYSTEM ARCHITECTURE

The researcher concluded that a case study was the most appropriate research methodology based on Gillham's [10] four underlying principles of a discrete human real world activity because the activity can only be understood in its context, it exists in the present, and its boundaries are not well defined in the context in which it exists. The article's author posed a research question, then constructed an exploratory case study to find an answer [11].

A. **Procedure for Conducting Work.** The researcher concluded that a case study of major American banks based in New Jersey would provide the most useful data for this work [12]. In order to recruit participants for the case study, the researcher contacted the heads of all the banks in New Jersey to ask for volunteers [13]. Senior bank officials familiar with their institution's cyber insurance and operational cyber risk mitigation measures [14] are the ideal participants for this research. Persons from the Office of the Chief Information Security Officer or a comparable bank entity, such as the Office of the Chief Risk Officer, were eligible to take part in a single in-person interview lasting one hour at the bank's location [15]. The worker is expected to be well-versed in all areas of cyber defence, including cyber insurance, for the financial institution.

B. Approach to Research. Since the researcher expected a limited sample size, she opted for mixed-methodologies research, which combines qualitative and quantitative methods to get a broader and deeper knowledge of the topic at hand and stronger supporting evidence [16]. The researcher relied on this definition in crafting the study's methodology. Data were gathered in one sitting using a structured interview instrument [17] devised for this study's cross-sectional case study research methodology [12]. The validity of both the qualitative explanations and the quantitative descriptions is enhanced

ISSN- 2394-5125 VOL 08, ISSUE 05, 2021

by the mixed-methods techniques utilised for this study [18], which is an improvement over the exploratory character of research in the social sciences.

C. **Information gathering.** Given the unique population under investigation, the delicate nature of the topic at hand, and the stringent criteria that needed to be followed in order to discover suitable participants, purposive sampling was used [17]. Officials from New Jersey banks listed on the State of New Jersey Department of Banking & Insurance public website were selected as participants because they represent a cross-section of the banking community at the time the research was conducted [13]. Individuals' bank branches served as the setting for the structured interviews employed in this research.

D. **Instrumentation.** As a means of gathering data, the study's investigator utilised predetermined sets of interview questions and predetermined answers. Programs and actions that reduce operational cyber risk were stood in for in this study using the NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, 2018. Operational cybersecurity risk mitigation programmatic requirements and particular cybersecurity actions are addressed by the NIST Cybersecurity Framework's 23 categories [3]. Based on these 23 classes, the researcher developed 33 unique, standardised questions for the survey. The 33-question test is structured according to the NIST Cybersecurity Framework's [3] five predetermined themes: identify; protect; detect; respond; and recover. The Baldrige Cybersecurity Excellence Builder [19] was used to produce a set of seven standardised replies. In addition to the 33 questions about operational cyber risk mitigation, the survey also included 12 questions about the participants' demographic information, such as their level of education, the type of bank they worked for, the bank's total assets under management, and whether or not the bank was actively using the NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. The cyber insurance research instrument concludes with nine structured questions that use predetermined answer options and inquire about the participant's bank's cyber insurance policies, industry developments, and technological innovations. Cyber risk insurance, cyber media liability insurance, cyber network security insurance, and cyber privacy insurance [7] form the basis for the first four insurance questions in this study, and the remaining five questions concern the amount of cyber insurance coverage your bank maintains, whether or not third-party contractors provide your IT and cybersecurity needs, the nature of your bank's cyber risk, and other related matters.

E. **Data Reporting process.** Since the sample size for the case study was too small to apply inferential statistics, a mixed-methods approach was used to analyse the data [12]. In order to perform the analysis, we first used Cronbach's alpha to check the code frequency distribution and make sure there was enough data saturation to make up for the low

ISSN- 2394-5125 VOL 08, ISSUE 05, 2021

number of participants [20]. As soon as a respectable Cronbach's alpha value was attained, a multi-method approach was taken to the data.

IV. RESULTS AND DISCUSSION

The purpose of this research was to ascertain whether or not significant banks in the United States's Garden State had improved their operational cyber risk mitigation as a result of purchasing cyber insurance. This study used an exploratory-triangulation [21] based case study research design.

A. **Data Collection Methodology.** To begin, we culled a list of 115 banks licenced to do business in New Jersey from the online database maintained by the state's Department of Banking and Insurance [13]. Fifteen of the 115 banks approached for this research declined to participate, while ten others replied positively to the research proposal invitation. All of the New Jersey institutions that took part in the research had acquired some kind of cyber insurance, and all of the banks included had total assets of more than $1 billion. New Jersey is home to 34 banks having assets in excess of $1 billion [13]. There was a 29% participation rate among the state's largest banks, defined as those with more than $1 billion in total assets.

Due to the small number of participants (10 big banks), we used Cronbach's alpha to determine whether or not our sample size was enough. Cronbach's alpha may be measured from 0.00 to 1.00, as stated by Marshall, Cardon, Poddar, and Fontenot [20], with an acceptable redundancy measurement of 0.70 being attained with as little as 9 interviews [22]. Participants 4 and 10 were interviewed, with Cronbach's alpha starting at 0.70 and ending at 1.00, respectively. Such a high Cronbach's alpha in so few interviews indicates a data collection with adequate homogeneity for future study [20] [22]. Cronbach's alpha, a measure of reliability, is compared against data saturation criterion in Figure 1.

B. **Findings from a Qualitative Analysis.** The homoscedasticity between the operational cyber risk mitigation factors and the cyber insurance variables was tested using a simple linear regression technique in the qualitative study [23]. A frequency measurement was used to identify the class frequency of each type of observation, and then the relative frequency was calculated by dividing the class frequency by the total number of observations in each dataset [24]. Table 1 displays the relative frequency analysis that was used to compare the nine independent factors to the six dependent variables qualitatively. Outcomes that are more than twice the random value are shown in green, while results that are more than three times the random value are shown in green (+ and ++). The findings are random at the top of Table 1 for the independent variable of cyber media liability insurance but become a mix of random and positive by the bottom independent variable of does your bank utilise a third party contractor(s) to fulfil its IT and cyber security requirements. The results appear to have a positive relationship with the six dependent variables of the identify function, the protection function, the detection function, the response function, the recovery function, and all five functions combined by the fourth independent

ISSN- 2394-5125 VOL 08, ISSUE 05, 2021

variable of whether or not your bank uses cloud computing services. The remaining five independent variables—the length of time a bank has been purchasing cyber risk insurance, the length of time a bank has been purchasing cyber network security insurance, the length of time a bank has been purchasing cyber privacy insurance, and whether or not a bank's cyber risk, cyber network security, or cyber privacy insurance coverage is first-party (purchased by the bank itself)—follow this pattern (with one exception).

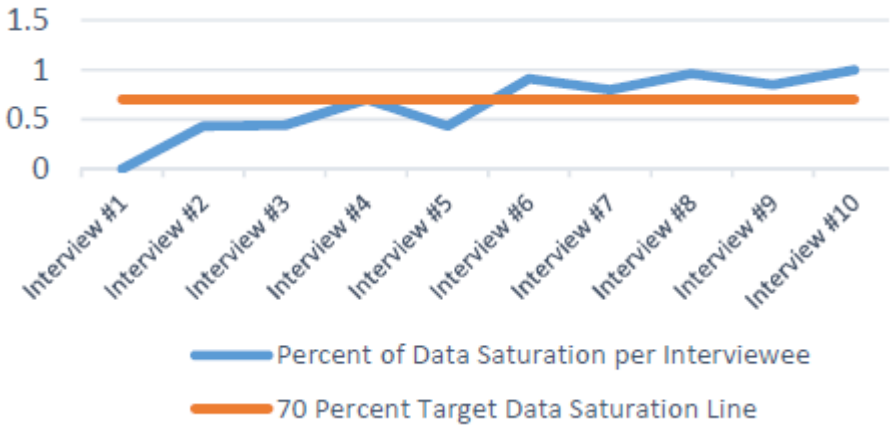

Fig.1 Data saturation criterion vs the cronbach's alpha reliability measure of duplicated replies.

C. **Findings and Quantitative Analysis.** Regression analysis was performed in the study's quantitative section to see whether the big banks in New Jersey's cybersecurity practises could be used to explain and forecast events outside of the study's context [12]. The study set out to use quantitative methods to show whether or not there was a measurable association between big banks in New Jersey's purchase of cyber insurance and improved operational cyber risk mitigation. Table 2 displays the quantitative findings from the regression coefficient analysis of the nine independent factors and the six dependent variables. Colors indicate the statistical significance of the data, with red indicating negative, yellow showing no statistical significance, and green indicating positive. The findings in Table 2 are negative and statistically significant starting with the independent variable of cyber media liability insurance and changing to positive, but not statistically significant, outcomes by the last three independent variables.

Statistically significant, but in a negative direction, are the four independent variables how long a bank has been buying cyber media insurance, how much cyber insurance coverage a bank has, whether or not a cloud computing service offers third-party cyber insurance coverage, and whether or not a bank uses cloud computing services. The findings of the fifth and sixth independent variables, the number of years your bank has been buying cyber network security insurance and the number of years your bank has been purchasing cyber risk insurance, were not statistically significant. Seventh through ninth independent variables how long your bank has

ISSN- 2394-5125 VOL 08, ISSUE 05, 2021

been buying cyber privacy insurance, whether or not your bank uses third-party contractors to supply your IT and cybersecurity needs, and whether or not your bank's cyber risk, cyber network security, or cyber privacy insurance coverage is first-party (purchased by the bank) or third-party (purchased by your contractor(s)) are all statistically significant and positive.

D. **Integration of Qualitative and Quantitative Findings.** With the triangulation phase complete, this research will have successfully used a mixed methods technique [21]. The researcher did this by comparing the findings from the qualitative and quantitative analyses [21]. Three of the nine independent cyber insurance variables meet both the qualitative and quantitative analyses criteria for a positive relationship that improves operational cyber risk mitigation in large banks in the State of New Jersey. The operational cyber risk mitigation variable is dependent on the three independent cyber insurance variables (the number of years a bank has purchased cyber privacy insurance; the use of third-party contractors to meet the bank's IT and cybersecurity needs; and whether a bank's cyber risk, cyber network security, or cyber privacy insurance coverage is first-party (purchased by the bank) or third-party (purchased by its contractors). Using criteria from the relative frequency and regression coefficient analyses, Table 3 compares the triangulation findings of the nine independent variables to the six dependent variables. When findings are negative and statistically significant, the bar will be red; when results are random and not statistically significant, the bar will be yellow; and when results are positive and statistically significant, the bar will be green. Triangulation findings are either random or negative, beginning with cyber media liability insurance at the top of Table 3. For the last three independent variables in Table 3, namely, how long your bank has been purchasing cyber privacy insurance, whether or not your bank's cyber risk, cyber network security, or cyber privacy insurance coverage is first-party (purchased by the bank) or third-party (purchased by your contractor(s)), the results progress from negative to random (or not statistically significant) to positive. and does your financial institution rely on outside vendors to meet its information technology and cyber security requirements?

E. **Synopsis of outcomes.** How long your bank has been acquiring cyber privacy insurance, whether or not your bank's cyber risk, cyber network security, or cyber privacy insurance coverage is first-party (bought by the bank) or third-party (purchased by your contractor(s)), are all separate cyber insurance factors. Both the qualitative and quantitative findings show that the dependent operational cyber risk mitigation factors in big banks in the State of New Jersey are improved when questions like "and does your bank utilise a third-party contractor(s) to meet your IT and cybersecurity needs?" are included.

ISSN- 2394-5125 VOL 08, ISSUE 05, 2021

TABLE I. Quality relative frequency analysis: a comparison

Cyber Insurance Variables	Operational Cyber Risk Function; Relative Frequency Methodology					
	Identify	*Protect*	*Detect*	*Respond*	*Recover*	*Combined*
Cyber Media Liability Insurance						
Total Cyber Insurance Coverage						
Cloud Computing Service Cyber Insurance Coverage						
Cloud Computing Service					+	
Cyber Risk Insurance				+	+	
Cyber Network Insurance				+	+	
Cyber Privacy Insurance			+	+		
Third Party Constructor(s) Cyber Insurance Coverage		+	+		+	
Third-Party Contractor(s)		++	+		+	+

TABLE II. Evaluations Of Quantitative Regression Coefficients

Cyber Insurance Variables	Operational Cyber Risk Function; Regression Coefficient Analysis					
	Identify	*Protect*	*Detect*	*Respond*	*Recover*	*Combined*
Cyber Media Liability Insurance	Negative	Negative	Negative	Negative	Negative	Negative
Total Cyber Insurance Coverage	Negative	Negative		Negative	Negative	Negative
Cloud Computing Service Cyber Insurance Coverage	Negative	Negative	Negative			Negative
Cloud Computing Service	Negative		Negative			Negative
Cyber Risk Insurance			Negative			
Cyber Network Insurance			Negative			
Cyber Privacy Insurance	positive	positive	positive	positive		positive
Third Party Constructor(s) Cyber Insurance Coverage	positive	positive	positive	positive	positive	positive
Third-Party Contractor(s)	positive	positive	positive	positive	positive	positive

TABLE III. Analyzing Regression and Relative Frequency Analysis The Outcome of the Coefficient Analysis

Cyber Insurance Variables	Operational Cyber Risk Function; Relative Frequency and Regression Coefficient Analyses Combined					
	Identify	*Protect*	*Detect*	*Respond*	*Recover*	*Combined*
Cyber Media Liability Insurance						
	Negative	Negative	Negative	Negative	Negative	Negative
Total Cyber Insurance Coverage						
	Negative	Negative		Negative	Negative	Negative
Cloud Computing Service Cyber Insurance Coverage						
	Negative	Negative	Negative			Negative
Cloud Computing Service					+	
	Negative		Negative			Negative
Cyber Risk Insurance				+	+	
			Negative			
Cyber Network Insurance				+	+	
			Negative			
Cyber Privacy Insurance			+	+		
	Positive	Positive	Positive	Positive		Positive
Third Party Constructor(s) Cyber Insurance Coverage		+	+		+	
	Positive	Positive	Positive	Positive	Positive	Positive
Third-Party Contractor(s)		++	+		+	+
	Positive	Positive	Positive	Positive	Positive	Positive

V. IMPLICATIONS OF RESULTS

There was a positive to very strong positive correlation between six of the nine independent variables and the six dependent variables. These six independent variables included the number of years a bank has had cyber risk insurance, the number of years it has had cyber

ISSN- 2394-5125 VOL 08, ISSUE 05, 2021

network security insurance, and the number of years it has had all five functions together (identify, protect, detect, respond, recover, and all five functions). Eight of the nine independent variables, including how long a bank has had cyber risk insurance, how long a bank has had cyber network security insurance, how long a bank has had cyber privacy insurance, how much cyber insurance coverage a bank has, whether or not a bank uses third-party contractors to meet its information technology and cybersecurity needs, and whether or not a bank's cyber risk, network security, and privacy insurance policies are all in force, are all significant. There may be a positive to very strong positive relationship between the other independent variables and at least one of the six outcomes (identify function, protection function, detection function, response function, recovery function, and all five functions combined), but the length of time your bank has purchased cyber media liability insurance seemed to have no bearing on any of the six dependent variables. While these results are informative for researchers, they don't provide practical guidance to bank managers since they don't address how cyber insurance impacts operational cyber risk mitigation at New Jersey's major banks.

A statistically significant negative connection or no link at all was found for six of the nine independent variables when regression coefficients were calculated using quantitative data from the six dependent variables and the nine independent variables. We ask six questions about each dependent variable: (a) how long has your bank been purchasing cyber media liability insurance; (b) how much cyber insurance coverage does your bank have; (c) does your cloud computing service provide your bank with third-party cyber insurance coverage; (d) does your bank use cloud computing services; and (e) how long has your bank been purchasing cyber network security insurance and cyber risk insurance. While these results may be of academic interest and practical value to bankers, they do not support the premise that the purchase of cyber insurance correlates positively with the decrease of operational cyber risk at large banks in the state of New Jersey.

The six quantitative results of the identify function, the protection function, the detection function, the response function, the recovery function, and the combination of all five functions are all positively and statistically significantly correlated, as shown by the regression coefficient analysis. Independent factors include the length of time a bank has been purchasing cyber privacy insurance, the usage of outside vendors to handle IT and cybersecurity tasks, and the purchase of first-party cyber risk, cyber network security, or cyber privacy insurance. The triangulation results provide credence to the theory that cyber insurance has a positive link with the lowering of operational cyber risk in large New Jersey institutions. These results are useful for both researchers in the academic realm and professional bankers in the actual world.

VI. SUGGESTIONS AND CONSTRAINTS

The research questionnaire was evaluated and edited by six experts from New Jersey's public and commercial sectors to guarantee its adequacy for examining the correlation between cyber

ISSN- 2394-5125 VOL 08, ISSUE 05, 2021

insurance and the enhancement of operational cyber risk mitigation in U.S. banks. The six experts also examined the questionnaire for reliability and internal validity, making sure that the questions would provide consistent results both inside the questionnaire and throughout time if the same people were surveyed again. Because there were just a few tweaks made to the interviews, we didn't bother with a pilot study. Since the NIST Cybersecurity Framework self-assessment instrument is so widely used throughout the nation, experts in the industry believed that the validity and reliability of the interview results would be high.

Credibility in the research comes from in-depth interviews that were done over the period of four months in the field [12]. This study was made possible by the author's interviews with New Jersey bank CISOs and others in comparable roles. Given that the participants in this case study [20] had similar features (high levels of education and training, substantial experience in cybersecurity, and federal or state regulation), the concept of data saturation was useful to compensate for the smaller sample size. This aided in determining an adequate sample size and checking the precision of the frequency distribution in the data, both of which are vital to the success of the research. Researchers often approach "data saturation," the assumption that fewer highly qualified participants are required before they would reproduce many of the same replies acquired from prior interviewers [20], a point of diminishing returns when little new data is given to the process.

A. **Limitations of The Work.** The lack of a Federal or State Department or Agency or National or State Banking Association to function as a trusted facilitator for outreach to possible sample participants and to help in presenting the researcher and this study to the target banking audience is the first limitation [25].

   In addition, most of the data pertaining to cybersecurity in banks is considered secret or proprietary [26, 27]. The researcher faced two additional challenges related to the sensitive nature of the data collection for this study: contextual, or the need to understand the environment in which the research is being conducted, in this case, large banks in the State of New Jersey; and personal security, or the need to ensure that the participants, senior cybersecurity personnel from banks, feel safe sharing information during interviews [26]. Third, the study's applicability was restricted by the fact that only 34 New Jersey banks with $1 billion or more in assets were included in the sample [13].

B. Delimitations of the Work. Information was only gathered for the state of New Jersey. It's true that New Jersey has a varied banking system, but there are several features of the Garden State's financial system and economy that aren't found in other states [27].

C. **Recommendations.** This study's results point to the need for additional involvement from federal, state, and private sector officials as well as banking industry top brass in fostering U.S. financial institutions' cyber resilience. The following are some recommended rules and procedures for improving bank cybersecurity in the United States: I'm talking about the a) Policy here. 1) The United States Government needs to

ensure that operational cyber risk is included in the calculation of minimum available regulatory capital requirements for banks. Two) Incentives for U.S. institutions to buy cyber risk insurance should be increased so that the banks would exhibit better enterprise-wide cyber risk management practises.Thirdly, the boards of directors and top executives of U.S. banks should establish rules that help the institutions assess their enterprise cyber risk and take the required steps to counteract the cyber threats to which they are most vulnerable. It's only a matter of b) getting some actual experience. 1) The boards of directors of banks in the United States should implement a plan for enterprise risk management that takes into account cyber risk and cybersecurity. 2) American financial institutions must pinpoint weaknesses in their enterprise risk management approach that compromise their privacy and safety online. Thirdly, financial institutions in the United States should develop a cyber strategy that takes into account their individual risk appetites and available resources.

VII. FUTURE SCOPE AND CONCLUSION

This case study provides evidence that both public and private actors may improve cybersecurity in US financial institutions. Greater collaboration between top executives from all key stakeholder groups is required to enhance enterprise risk management throughout the banking industry as a whole. This research is the first of its kind to utilise real-world data to evaluate the premise that U.S. banks might reduce their operational cyber risk by purchasing cyber insurance. To further this line of inquiry, future studies should replicate this kind of cross-sectional analysis in other regions of the country and with different types of financial institutions. Qualitative research approaches, such as semi-structured or unstructured interviews, focus groups, and the more common one-on-one, structured interviews, may provide light on the nuances of issues like purchasing cyber insurance and enhancing operational cyber risk mitigation programmes and activities. If these preliminary follow-up steps prove fruitful, it is recommended that a switch be made from smaller, purposive sampling to larger, random sampling of the U.S. banking industry in order to further validate the findings of this study and allow for broader generalisations to the larger population of U.S. banks while addressing earlier biases in the research. Given the dynamic and ever-changing nature of cyber risk, further longitudinal studies incorporating some of the original study participants to see whether the results hold true over time or have evolved to meet a new cyber risk environment should be addressed.

REFERENCES

[1] C. Biener, M. Eling, and J. H. Wirfs, 2015. Insurability of cyber risk: An empirical analysis. *The Geneva Papers on Risk and Insurance-Issues and Practice*, *40*(1), pp.131-158.

[2] B. Carin, 2017. G20 safeguards digital economy vulnerabilities with a financial sector focus. *Economics*, *11*(1).

[3] M.P. Barrett, 2018. Framework for improving critical infrastructure cybersecurity version 1.1.

[4] C. Moschovitis, 2018. *Cybersecurity Program Development for Business: The Essential Planning Guide*. John Wiley & Sons.

[5] R. Q. Hahn and A. Layne-Farrar, 2006. The law and economics of software security. *Harv. JL & Pub. Pol'y*, *30*, p.283.

[6] D. W. Hubbard, and R. Seiersen, 2016. *How to measure anything in cybersecurity risk*. John Wiley & Sons.

[7] L.A. Odell, J. C. Fauntleroy, and R. R. Wagner, 2015. Cyber Insurance– Managing Cyber Risk. *Institute for Defense Analyses, April*.

[8] K. Dandapani, 2008. Growth of e- financial services: Introduction to the special issue. *Managerial Finance*

[9] Healey, J., Mosser, P., Rosen, K. and Tache, A., 2018. The Future of Financial Stability and Cyber Risk. *The Brookings Institution Cybersecurity Project*, pp.1-18.

[10] B. Gillham, 2000. *Case study research methods*. Bloomsbury Publishing.

[11] Y.C. Gagnon, 2010. *The case study as research method: A practical handbook*. PUQ.

[12] J. Rudolph, P.D. Leedy, & J. E. Ormrod, (2015). Practical research. Planning and design . Boston, MA: Pearson. *Journal of Applied Learning and Teaching*, *1*(2), pp.73-74.

[13] State of New Jersey, Department of Banking & Insurance (NJDOBI) website. (2018). New Jersey Financial Institutions. Retrieved from https://www.state.nj.us/dobi/bankwebinfo.htm

[14] Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC). (2016). Purchasers' Guide to Cyber Insurance Products, 1-26. Retrieved from https://www.fsscc.org/files/galleries/FSSCC_Cyber_Insurance_Purchasers_Guide_FINAL-TLP_White.pdf.

[15] J. Fruhlinger, J. (2019). What is a CISO? Responsibilities and requirements for this vital leadership role. *CSOonline.com*, Jan 14, 2019 at 3:00 am PST. Retrieved from https://www.csoonline.com/article/3332026/what-is-a-cisoresponsibilities-and-requirements-for-this-vital- leadership-role.html

[16] P. M. Daigneault and S. Jacob, 2014. Unexpected but most welcome: Mixed methods for the validation and revision of the participatory evaluation measurement instrument. *Journal of Mixed Methods Research*, *8*(1), pp.6-24.

[17] J. W. Creswell and J. D. Creswell., 2017. *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.

[18] J. Stolz, A. Lindemann, and J. P. Antonietti, 2019. Sociological explanation and mixed methods: the example of the Titanic. *Quality & Quantity*, *53*(3), pp.1623-1643.

[19] U.S. Department of Commerce, National Institute of Standards and Technology (NIST). (n.d.). *Baldrige Cybersecurity Excellence Builder*, 1-32. Retrieved from

https://www.nist.gov/sites/default/files/documents/2017/04/03/baldrigecybersecurity-excellence-builder-1.0.pdf

[20] B. Marshall, P. Cardon, A. Poddar, and R. Fontenot, 2013. Does sample size matter in qualitative research?: A review of qualitative interviews in IS research. *Journal of computer information systems*, *54*(1), pp.11-22.

[21] L. Kwok, 2012. Exploratory-triangulation design in mixed methods studies: A case of examining graduating seniors who meet hospitality recruiters' selection criteria. *Tourism and Hospitality Research*, *12*(3), pp.125-138.

[22] M. M. Hennink, B. N. Kaiser, and V. C. Marconi, 2017. Code saturation versus meaning saturation: how many interviews are enough?. *Qualitative health research*, *27*(4), pp.591-608.

[23] T. H. Wonnacott, 1981. *Regression; a second course in statistics* (No. 04; QA278. 2, W6.).

[24] R. L. Ott and M. T. Longnecker, 2015. *An introduction to statistical methods and data analysis*. Cengage Learning.

[25] G. S. ed. Szarycz, 2010. *Research realities in the social sciences: Negotiating fieldwork dilemmas*. Cambria Press.

[26] C.M. Renzetti and R.M. Lee, 1993. Researching sensitive topics. Newbury Park, CA: SAGE Publications, Inc.

[27] J. Ritchie, J. Lewis, C. M. Nicholls, and R. eds. Ormston, 2013. *Qualitative research practice: A guide for social science students and researchers*. sage.