ECONOMIC ANALYSIS OF CYBER RISK FOR FINANCIAL INSTITUTIONS

- Avisha Gupta[1], Dr. Chitra Saruparia[2] , Dr. Arun Kumar Giri[3],

ABSTRACT

Cyberattacks have surged rapidly during the previous five years, and cybersecurity experts anticipate one attack every 11 seconds by 2023. Financial stability is under risk owing to the ease with which attackers can cause massive upheaval to the IT infrastructure technology systems utilised by banking firms. Cyberattacks and data breaches have risen from being an IT unit concern to being a key risk management issue for all financial institutions. The importance of safeguarding information systems to maintain commercial and financial activity in a firm has grown in the wake of the COVID-19 pandemic. By analyzing the 10-K filings of the US-listed firms and statistics on cybercrimes, the objective of this study is to propose a novel cyber risk measure for publicly traded US firms. According to our analysis, the financial sector is unprepared for such attacks, and the international community is responding in a disjointed fashion. Our measure's time-series properties correlate with cyberattacks, as indicated by a 0.83 positive correlation between our measure and the annual cyberattack percentage. The study is a step towards developing a standardized global cyber risk measure for the banking industry.

Keywords: *Cyber-incidents, Operational risk, Basel Committee, SEC Edgar, Advisen data, Cybersecurity risk measure, National Cyber Security Index, Banking industry, Technology advancement, Cyber risk insurance.*

[1] Master Student, Department of Economics and Finance, Birla Institute of Technology and Science (BITS), Pilani, Rajasthan,
[2] Assistant Professor (Economics), Faculty of Humanities and Social Sciences, National Law University, Jodhpur
[3] Professor, Department of Economics and Finance, Birla Institute of Technology and Science (BITS), Pilani, Rajasthan, India,

1. INTRODUCTION

Any potential for monetary loss, disruption, or damage to an organization's reputation due to the malfunction, unauthorized use, or inadvertent misuse of its information systems is considered a cyber risk. As the number, scale, and sophistication of cyberattacks on the world's financial institutions increase, the threat they pose can no longer be dismissed as media hype. Cybersecurity experts predict that in 2023, there will be a cyberattack every 11 seconds, which has exponentially increased since the last five years. Private data of several clients has been exposed due to hacks of major banks, credit bureaus, and government entities. When financial institutions use third-party service providers, any data breaches on the part of those suppliers pose a serious threat to the privacy and proprietary information of the institutions. The advent of globalization of economies, the use and widespread acceptance of rapidly evolving technologies, the extensive interdependences and interrelations between the financial sector and the IT infrastructure, the increasing sophistication of malicious actors, and the fundamental nature of banking institutions' businesses and services all contribute to the cyber risk that these organisations face. However, the financial sector's ability to assess and analyze cyber risk has not yet developed to the level at which it can be regularly monitored against business risk sensitivities or assessed from a system-wide standpoint. In consequence of this, entities' collective and individual preparedness to deal with system-level cyber threats is diminished, as is the effectiveness with which such risk is measured and managed.

Another significant source of cyber risk for financial institutions is the “dark web”, a web of anonymous activity and hidden pages that cannot be followed. This is due to the fact that businesses desire complete anonymity in the event that an incident does occur, as they do not prefer for it to be reported in the media, and moreover, they may be victims of dark web activity without even realizing it. Information such as bank statements and card numbers can be posted as a link and exploited in this setting. Many businesses have a hard time tracking down thieves because of how simple it is to gain access to the dark web and how little evidence their actions leave behind. A crucial observation to make here is that this is something of a murky area, since targeted financial institutions are typically reticent to disclose how they learned of the attack, which might occasionally be through reconnaissance of the dark web. It's important to note that

banks and other financial institutions aren't slacking off when it comes to managing cybersecurity risks; in fact, they're taking a more nuanced approach than many businesses in other industries, particularly the retail sector.

The objective of this study is to conduct an economic analysis of cyber risks and propose a novel cybersecurity risk measure for US-listed firms based on a textual analysis of firms' disclosures and available data on cyber-attack incidents. A significant issue that most organizations face while disclosing the operational risks involved is the absence of a standardized definition and classification of cyber risks. Cyber risk can be defined in a variety of ways depending on the setting. Cyber risk, as defined by the ORX's Cyber and Information Security Risk project, is the potential for monetary or other types of loss as a result of cyber incidents that have either an external or internal source.[1] Cyberthreats and their inherent causes would be easier to comprehend with a standardized description and classification. Data sharing and proper collaboration in managing cyber risks might be facilitated even more by a unified set of definitions and an agreed upon understanding across the finance industry, both among regulatory authorities and private entities. So, we base our definition off of what the Basel Committee for Banking Supervision has proposed, which is stated in the following section. Our analysis also presents different patterns of cyber-attacks each industry faces and provides measures for a faster response and recovery. The final section of the report mentions existing campaigns and programs that strengthen the cybersecurity infrastructure and raise awareness among organizations. Moreover, the section suggests policies and strategies that can be put in place to improve response to and recovery from the cyber-attack.

2. RATIONALE OF ECONOMIC ANALYSIS OF CYBER RISK FOR FINANCIAL INSTITUTIONS IN LEGAL LANDSCAPE

Financial institutions are frequently targeted by hostile individuals causing disruption since they hold enormous volumes of sensitive financial data. In the financial sector, cyber-attacks can have a negative impact on the economy through direct financial losses, reputational harm, operational

[1] Luke Carrick et al., *An emergent taxonomy for operational risk: capturing the wisdom of crowds*, 15 Journal of Operational Risk (2020).

implications, insurance concerns, regulatory compliance costs, systemic risk, and long-term effects on shareholders and investors. Consequently, the legal context's economic analysis of cyber risk for financial institutions entails a comprehensive investigation of the direct and indirect expenses linked to cyberthreats as well as various strategies for mitigating such costs. In globalized world, financial institutions must constantly adapt and invest to protect their reputation and financial viability due to the ever-evolving nature of cyber threats. In this way from the lens of economics we can say that cybercrimes and attacks are market failures which cause huge cost to the society; that can be mitigated by investments in cyber security. Such investments lead positive externalities to the society and exhibit characteristics of public good. Laws and legal framework can play a conducive role to correct market failure in ensuring cyber security. Hence there is justification for discussing the economic analysis of cyber risk for financial institutions in the legal landscape. In addition to this, intersection of law and economics of cyber security is considered to be as a fertile ground for contributions to cyber security. Given the complexity and prevalence of cyber risks in the digital era, financial institutions must undertake an economic analysis of cyber risk. However, little research is done on economic analysis of cyber risk but relatively there are very few research on the role of law and legal institutions in the economics of cyber security. Our research was carried out with the objective of developing a novel cybersecurity risk measure, describing the numerous cyberattack patterns that are specific to each industry, as well as the strategies that can be put in place to ensure an efficient response and recovery from any attacks.

3. REVIEW OF LITERATURE

Bank risks are multifaceted, and system errors, frauds, legal suits, and operation disruptions are just some of the hazards that have historically been associated with operational failures in the banking sector. These dangers have always existed in the banking industry. According to the FDIC's article, one of the great challenges in systematically managing these types of risks is that operational losses can be quite diverse in their nature and highly unpredictable in their overall financial impact.[2] The conventional banking tools used[1] to counteract operational risks are not

[2] Operational risk management: an evolving discipline, FDIC (Mar. 12, 2024, 13.55PM) https://www.fdic.gov/regulations/examinations/supervisory/insights/sisum06/sisummer2006-article01.html

enough with the evolving complexity in the finance industry. Operational risk management has grown as a discipline to become of paramount importance with several large operational losses and a changing capital regime in recent years.

When Basel I was adopted in 1988, it lacked a charge specifically for operational risk. It could be argued that operational risk and other risks were implicitly accounted for in the calibration of the minimum ratio thresholds for the various Prompt Correction Action categories, but they are not considered in determining a bank's capital ratios.[3] With increase in the number and amount of operational losses in financial institutions, the need for a fundamental strengthening of the existing framework had become apparent. Thus, the Basel II accord was proposed, incorporating operational risk into regulatory capital, and the Basel Committee for Banking Supervision established the following definition:

"Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events".[4]

Under this framework, firms (both mandatory and opt-in) were required to include an operational risk charge in their risk-weighted assets calculation alongside credit risk and market risk charges.[5] This led to operation risk exposure for a firm, directly affecting its risk-based capital ratio. Following are the three different approaches to determining operating risk capital charges laid forth in the Basel II accord, with increasing levels of sophistication and risk sensitivity between them: Basic Indicator Approach (BIA); Standardized Approach (SA); and Advanced Measurement Approach (AMA). Under the BIA, banks simply have to keep in the form of capital at least 15% of their revenues, while in the SMA calculation, this percentage is not fixed at 15% but varies according to the different business lines. The AMA applies external and internal data to value-at-risk methods that have to be validated by the supervisory authority.[6]

Further, the Basel Committee has identified seven operational risk event types: internal fraud, external fraud, employment practices and workplace safety, clients, products, and business practices; damage to physical assets; business disruption and system failures; execution, delivery,

[hereinafter "Operational Risk, FDIC"].

[3] *Id.*

[4] Basel committee on banking supervision, *Principles for Sound Liquidity Risk Management and Supervision (September 2008),* https://www.bis.org/publ/bcbs144.html (last visited March 13, 2024).

[5] *Id.*

[6] Basel Committee on Banking Supervision, *Basel II: International Convergence of Capital Measurement and Capital Standards: a Revised Framework* (June 2004) http://www. bis. org/publ/bcbs.html (last visited March 13, 2024).

and process management.[7] These are considered Level I loss categories, which are generally used by many studies while conducting empirical analysis. Moreover, Basel II also provides a subdivision of each loss category into further event types (Level II), which studies[8] also consider as a proxy for cyber-related events.

During 2008 and the years that followed, new understanding was obtained on the importance of operational risk management to the banking industry as well as the most effective strategy to manage these risks. It put forth the weaknesses of the banking sector, which had too much leverage and inadequate liquidity buffers to cover systematic risks that are derived from huge credit losses and were accompanied by poor governance and risk management.[9] According to Berger's research, operational risk at big bank-holding businesses in the United States is empirically linked in a favorable way to traditional metrics of financial systemic risk.[10] The great financial crisis thus led to the formulation of the Basel III accord, which streamlines the operational risk framework by proposing AMA and the existing three measuring strategies to be replaced by a single, risk-sensitive, standardized measurement strategy (SMA).[11]

In response to more risks rising from evolving bank operating models, a BCG article[12] presents increased spending on OR (operational risk) management by banks by more than 50% since 2010. However, the effectiveness of these investments by the boards and executive teams seems obscure. Further, the article lays down some steps for institutions to help them build a leading operational risk program that involves creating clarity around OR goals, addressing critical obstacles to achieving the bank's OR goals, and building a set of OR competencies.

Aldasoro et al. (2020)[13] observe a decrease in operational losses in recent years after a sharp

---

[7] Basel committee on banking supervision, *QIS 2 - Operational Risk Loss Data (May 2001)* https://www.bis.org/bcbs/qisoprisknote.pdf (last visited March 13, 2024).

[8] Operational Risk, FDIC, *supra* at 2; Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T., *Operational and cyber risks in the financial sector*, BIS Working Paper No. 2020/840 (2020). [hereinafter "Aldasoro"].

[9] Abdullah Ahmed Aloqad et al., Operational Risk Management in Financial Institutions: An Overview, 8(2) Business and Economic Research (2008).

[10] Bergera, A. N., Curtib, F., Mihovb, A., & Sedunovc, J. (2018). Operational Risk is More Systemic than You Think: Evidence from US Bank Holding Companies. Allen N. Berger et al., *Operational Risk is More Systemic than You Think: Evidence from US Bank Holding Companies,* Journal of Banking & Finance (2021).

[11] Penikas, H., *History of banking regulation as developed by the Basel Committee on Banking Supervision 1974-2014*. Banco de Espana 1, 9-47 (2015), https://www.semanticscholar.org/paper/History-of-Banking-Regulation-as-Developed-by-the-Penikas/740846b42fe110a77d17e3ad9345e93b247e8e9d.

[12] Bickford, J. K., Grüter, M. D., Le Boulay, G., Martin, D., & O'Malley, B., *The five practices that set operational risk leaders apart*, BCG (Mar 11, 2024, 4.24 PM) https://www.bcg.com/publications/2016/financial-institutions-operations-five-practices-operational-risk-leaders-apart. [hereinafter "Bickford"]

[13] Aldasoro, *supra* note at 8.

increase after the global crisis in 2008. The study conducts a cyber incident-level cross-country investigation to record the evolution and characteristics of operational risk in financial institutions worldwide. This study contributes to the current body of research by conducting an analysis on the interdependencies of the macroeconomic variables and operational risks involved. In order to accomplish this, it complements the data on operational risk with data from other sources. This data demonstrates that bigger operational losses occur following booms in the business cycle and favorable monetary policy. The paper puts forward evidence that, on average, operational losses take more than a year to be discovered and recognized in the books. Also, it finds heterogeneity in the time of discovery and recognition of losses and states the reason for that to be inconsistency in the implementation of the Basel framework across regions.

Cyber risks can be viewed as a subset of operational risks. When it comes to the regulation of cyber risk in the banking industry, Kashyap and Wetherilt (2019) present some concepts that regulators should take into consideration. In addition, the Basel Committee has developed regulations for financial institutions concerning the best practices for managing cyber risk. In March 2017, the G20 Finance Ministers and Central Bank Governors noted that "the malicious use of information and communication technologies (ICT) could disrupt financial services crucial to both national and international financial systems, undermine security and confidence, and endanger financial stability".[14]

In addition, Aldasoro et al. (2020) present an estimate of losses caused by cyber events. They do this by developing a substitute for cybercrimes based on the classification of various instances in the ORX database.[15]

According to the findings of the article, although cyber losses make up a relatively insignificant portion of total operational losses, they are nonetheless responsible for a sizeable portion of the total value that is at risk.

According to a cross-industry study conducted by Romanosky, S. (2016), 51% of the recurrent victim firms of cyber attacks belong to the finance and insurance sectors.[16] The study also contends that despite the fact that businesses in the financial sector are subject to stringent

[14] G20 Information Centre, http://www.g20.utoronto.ca/2017/170318-finance-en.html (last visited at Mar 13, 2024).
[15] Bickford *supra* at, 12.
[16] Romanosky S., *Examining the costs and causes of cyber incidents*, 2(2) JOURNAL OF CYBERSECURITY 121-135, (2016). [hereinafter "Romanosky"].

regulations regarding the controls they must implement to ensure data security, these businesses do not appear to be able to withstand cybercrime or minimize the losses in a monetarily superior manner compared to businesses in other industries. However, a limitation to this argument is that the study doesn't take into account how severe the attacks were that were waged against the companies in the business. Further, the study demonstrates that the total expenditures of the breaches only account for 0.4% of the company's revenues, which is a substantially lower percentage than the losses that are incurred as a result of other factors such as fraud, theft, corruption, or bad debt.[17] This lends credence to the idea that public issues concerning the rising frequencies of cybersecurity incidents and law suits may be exaggerated in comparison to the relatively little financial consequences that these occurrences have on the companies that are affected by them.

Bouveret, A. (2018)[18] recognizes cyber risk as one of the primary threats to financial stability by documenting different types of cyber attacks on financial institutions around the world and identifying their patterns, while also presenting a quantitative framework to assess these risks. The paper outlines the three factors that make financial institutions more vulnerable to cyber risks - high threat levels due to proxy organizations[19] and monitoring of communications carried out by unauthorised persons, increased opportunities for malicious activity on the internet because of dependencies on densely interconnected networks; potentially significant repercussions as a result of these accidents due to the immaterial nature of financial activity, which is primarily dependent on technological advancements. Further, it presents an empirical analysis yielding estimates and distribution of aggregate financial system losses due to cyber-attacks. The study analyzes ORX News data on cyberattacks to assess immediately incurred financial losses; nonetheless, damage to the firm's reputation due to a cyber incident is not addressed because it is customarily omitted from the risk disclosure and then adjusted for inflation to make it comparable across time. A primary limitation of this framework was the absence of complete data and differences in the definition of cyber risks across countries. An article by McKinsey also mentions that the distinguishing definitions of the roles of the operational-risk function and other oversight

[17] *Id.*
[18] Bouveret, A., Cyber risk for the financial sector: A framework for quantitative assessment. IMF Working Paper No. 2018/143 (2018).
[19] Kopp, E., L. Kaffenberger, C. Wilson, *Cyber Risk, Market Failures, and Financial Stability*, IMF Working Paper No. 2017/185 (2017).

groups—especially compliance, financial crime, cyber risk, and IT risk—have been fluid. But this constraint has been lifted in recent years with granular data and measurement on operational processes, employee activity, customer feedback, and other sources of insight widely available.

4. DATA AND METHODOLOGY

4.1 Constructing Cyber Security Risk Measure (US-listed firms)

As businesses have become more reliant on IT infrastructure, the threat posed by cybercriminals has grown in tandem. Companies in the US are obligated by the SEC Regulations to disclose the impact on their operations posed by cybersecurity risk in the "Item 1A. Risk Factors" section of their 10-Ks. The SEC published explicit rules in 2011 and 2018 requiring public businesses to inform their investors in a timely, comprehensive, and accurate manner about significant cybersecurity risks and incidents.[20] The guidelines apply to both firms that have been attacked and those that face major cybersecurity threats but have not yet been attacked. To draw a textual analysis of the cyber-related incidents, we used Python to download every 10-K form filing from SEC Edgar[3], except revised papers, and filter the cybersecurity risk disclosures from "Item 1A. Risk Factors". Further, it is implicit that the extracted information will have terms representing cybersecurity risk directly as well as indirectly. So, in the first phase of data processing, we develop and deploy a list of terms that directly represent cybersecurity risk. We then look for other relevant or irrelevant keywords within the same sentence to decrease the noise caused by the key terms and phrases in the disclosures that are unrelated to the risk associated with cybersecurity. Companies may address their security precautions, confirmed data disclosures, and the effects a cyberattack could have in indirect references. We then construct a new list of oblique keywords and phrases to locate the relevant lines, classified based on the potential legal and financial impacts. Organizations usually mention explicit cyber risk mitigation measures, and discuss the risk associated with a potential cyber attack along with its cybersecurity risk exposure in cybersecurity risk disclosures. Moreover, the information included in these disclosures fails to account for firm-specific,

[20] U.S. Securities and Exchange Commission, https://www.sec.gov/news/public-statement/statement-stein-2018-02-21 (last visited Oct 13, 2024); U.S. Securities and Exchange Commission, https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.html (last visited Oct 13, 2024).

nonsystematic risk, which financial markets may not have the ability to value. As a result, constructing a measure of cybersecurity risk at the business level is challenging, and thus we constructed a sample that only included companies that had suffered a severe cyberattack. In order to measure vulnerability to cyberattacks, we plan to estimate how closely each company's disclosure of cybersecurity risk resembles those of companies in the constructed sample, which also allows us to focus.

We used the extracted textual information to build the cybersecurity risk indicator. The metric considers how closely each company's disclosure of cybersecurity risk matches previous disclosures by companies in our training sample. It is anticipated that companies whose perceived risk and its mitigation employ comparable strategies are similarly susceptible to cyberattacks. We used separate word vectors to store the text rather than the actual words themselves after removing words that are irrelevant to our analysis (like stopwords, nouns, and pronouns). We then use this vector of 4,120 words to calculate the degree of similarity between any two 10-K filings by measuring the number of times each keyword occurs in the text.

Next, we compute the most common similarity measuring metrics, Jaccard and Cosine similarity, for each year for every company with all N_{t-1} disclosures of companies that were hit by cyberattacks in the year leading up to the reporting date for that particular firm and year in our training sample.

Jaccard similarity is calculated by dividing the intersection of two vectors by their union.

$$\text{Jaccard Similarity} = \frac{A \cap B}{A \cup B}$$

----- 25]

Cosine similarity is a measure of how closely two vectors are aligned, based on the cosine of the angle between them. This is calculated as:[21]

$$\text{Cosine Similarity} = \frac{A \cdot B}{||A||\,||B||} = \frac{\sum_{i=1}^{n} A_i B_i}{\sqrt{\sum_{i=1}^{n} A_i^2}\sqrt{\sum_{i=1}^{n} B_i^2}}$$

The significant difference between the two-similarity metrics is that Jaccard similarity accounts

[21] Sanket Gupta, *Overview of Text Similarity Metrics in Python*, TOWARDS DATA SCIENCE (Mar 11, 2024, 12.08 PM) https://towardsdatascience.com/overview-of-text-similarity-metrics/.

only for unique words in the word vector, while the cosine similarity method considers the total length of the word vector. Thus, Jaccard serves as a good measure where we do not consider repetition of words, while cosine similarity accounts for the duplication.

$$\text{Cybersecurity Risk Measure (i, t)} = \sum_{n=1}^{N} \frac{Cosine\ Similarity\ (i,n,t)}{N_{t-1}}$$

Similarity values for the Cosine and Jaccard methods are in the set [0, 1], with higher scores indicating a closer similarity in the disclosures. Since we do want to consider the repetition of the words in the similarity metric, we characterize the level of cybersecurity risk for each firm and year as the average cosine similarity across all N_{t-1} similarities as shown above.

4.2 Descriptive Cyber Loss Data for Cross Country Analysis

Advisen, a for-profit American firm that compiles and redistributes loss and event data to the commercial insurance sector on a wide variety of corporate loss types, has compiled a dataset of cyber occurrences.[22] The cyber loss data offered by Advisen presents a historical perspective on more than 90,000 cyber events, which include conflict occurrences, and was compiled using trustworthy and publicly verified sources. Each occurrence has been traced back to its parent business and possesses one or more of the following characteristics: case type, its status, source and type of loss, loss amount, and details of the affected company.[23]

Factiva was used to verify the cyber occurrences and narrow them down to those that were covered by major news articles throughout the world.

5. RESULTS AND DISCUSSION

5.1 Cybersecurity risk Measure for US-listed Financial Firms

As a result of growing public awareness of the dangers posed by cyber incidents, it can be seen that leaders and regulators around the globe have taken measures to reduce cybersecurity risks at

[22] Romanosky, *supra* at 17.
[23] Advisen Limited, https://www.advisenltd.com/data/cyber-loss-data/ (last visited Mar 10, 9.58 PM).

financial firms, such as improving resilience capabilities and formulating policies for impactful recovery and response from cyberattacks. Furthermore, it is not wrong to anticipate that firms with greater cybersecurity risk exposure will take concrete measures to actively manage that risk, and buying cyber insurance is one of those measures. Thus, in our textual analysis, we actively searched the word "insurance" and found a significant share of 9.24% of all the companies collectively in our sample. We also validated our assumption by verifying that approximately 77% of the firms had a cybersecurity risk measure (calculation done as described in Section 3.1) way above the median.

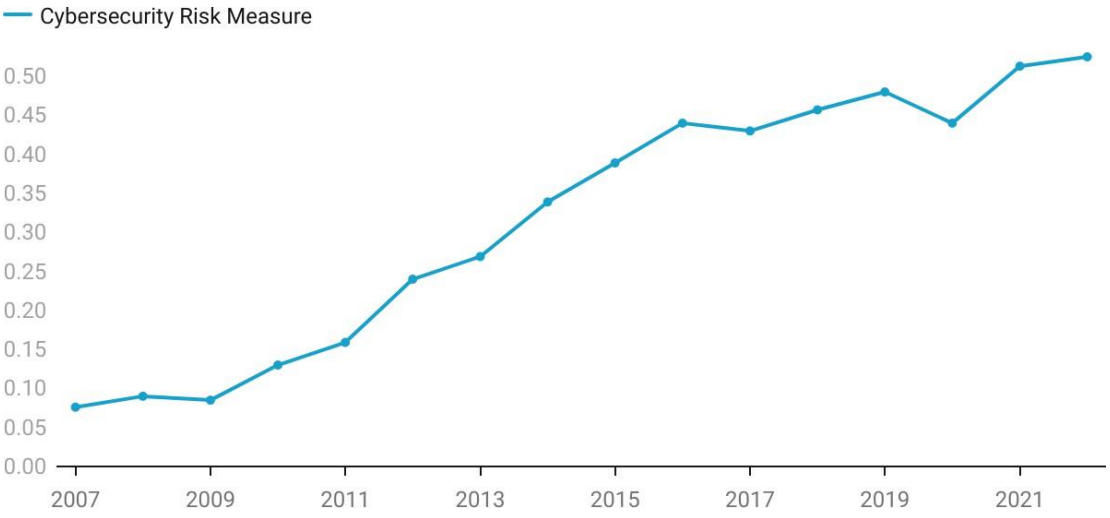


Fig. 1. Time Trend of Cybersecurity Risk Meaure (US-listed financial firms).
Source: Author's construction.

The accompanying chart (Fig. 1) presents the yearly trend of the constructed cybersecurity risk measure for the financial firms listed in the US. Positive trends over time are evident from the figure, with a sharp rise after 2011. This is because the SEC asked US firms to disclose their cyber risk exposures in 2011. Additionally, in the same year, 51.23% of the firms showed no cybersecurity risk, while only 11.95% of them did in 2021. Increased cyber threats during this time period can be traced back to the several successful cyberattacks that have been launched against publicly traded companies. A positive correlation of 0.83 between our measure and the annual cyberattacks percentage suggests that our measure's time-series features correlate closely to the count of cyber.

5.2 Cross-Industry Analysis (US-listed firms)

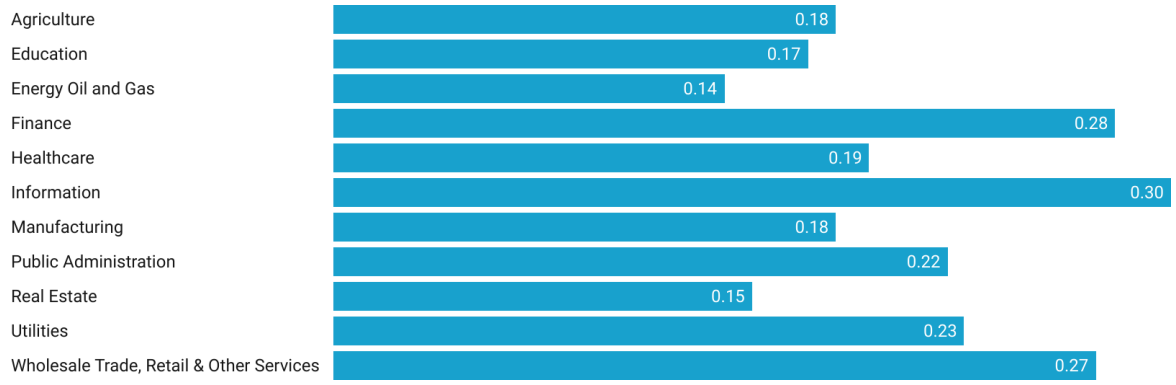


Fig. 2. Cross-industry analysis of Cybersecurity Risk Measure (US-listed financial firms). Source: Author's construction.

The above figure presents the calculated cybersecurity risk measure for the US-listed firms, categorized and averaged on the basis of the industry they belong to. It is evident that the finance and information industry ranks top across industries. Further, after analyzing the data points over the years, we find that the IT, retail, and financial sectors have been representing the greatest risk over the years, whilst the health and educational services sectors have some of the lowest risks. The results are also consistent with the Advisen data, which comprises the number of cyber attacks and data breaches, where the finance industry reported the highest number of cybercrimes among industries, along with the manufacturing and education sectors. This might be because of their shared reliance on IT; all of these sectors are particularly susceptible to cybercrime. The sophistication of cybercrimes as well as firms' exposure to this risk are rising, and it can be inferred that businesses in sectors that are more dependent on IT are more vulnerable to cyberattacks.

5.3 Identifying Patterns of Cyber Attacks

This section talks about the focus areas of cyber security incidents and puts forth a breakdown of around 5,000 verified cyber incidents and data breaches for a better analysis of the parameters involved. Because no two industries are the same, cyber incidents and breaches are classified by

industry. The study is based on the fact that the types of assaults suffered by a specific industry will depend heavily on the infrastructure they rely on, the data they manage, and the manner in which their customers, employees, and other stakeholders engage with them. For example, a huge corporation whose business strategy is based solely on mobile devices and whose consumers use an app on their smartphones will face different dangers than a small mom-and-pop store with no internet presence that uses a point-of-sale provider to manage its systems. Thus, the infrastructure and, conversely, the attack surface determine the risk to a great extent, which cautions people not to jump to conclusions about the security posture solely based on the number of reported breaches or incidents.

Before moving on to the analysis, it is important to realize that despite the close relationship between security incident and breach, they are distinct security terms. A security incident is any lapse in an organization's security measures, while a security breach is when an outsider gains access to otherwise secure areas of an organization and uses that access to commit fraud or expose private information. In many cases, incidents and data breaches go hand in hand, with the majority of breaches occurring after an incident. Consequently, preventing this transition is critically important for the success of a security plan, where it is implicit that organizations with more safeguards in place to stymie or halt an attack have a better security posture. The graphs below (Fig. 3, 4) show trends in cyber-incidents and breach rates, as well as provide an overview of different industries.

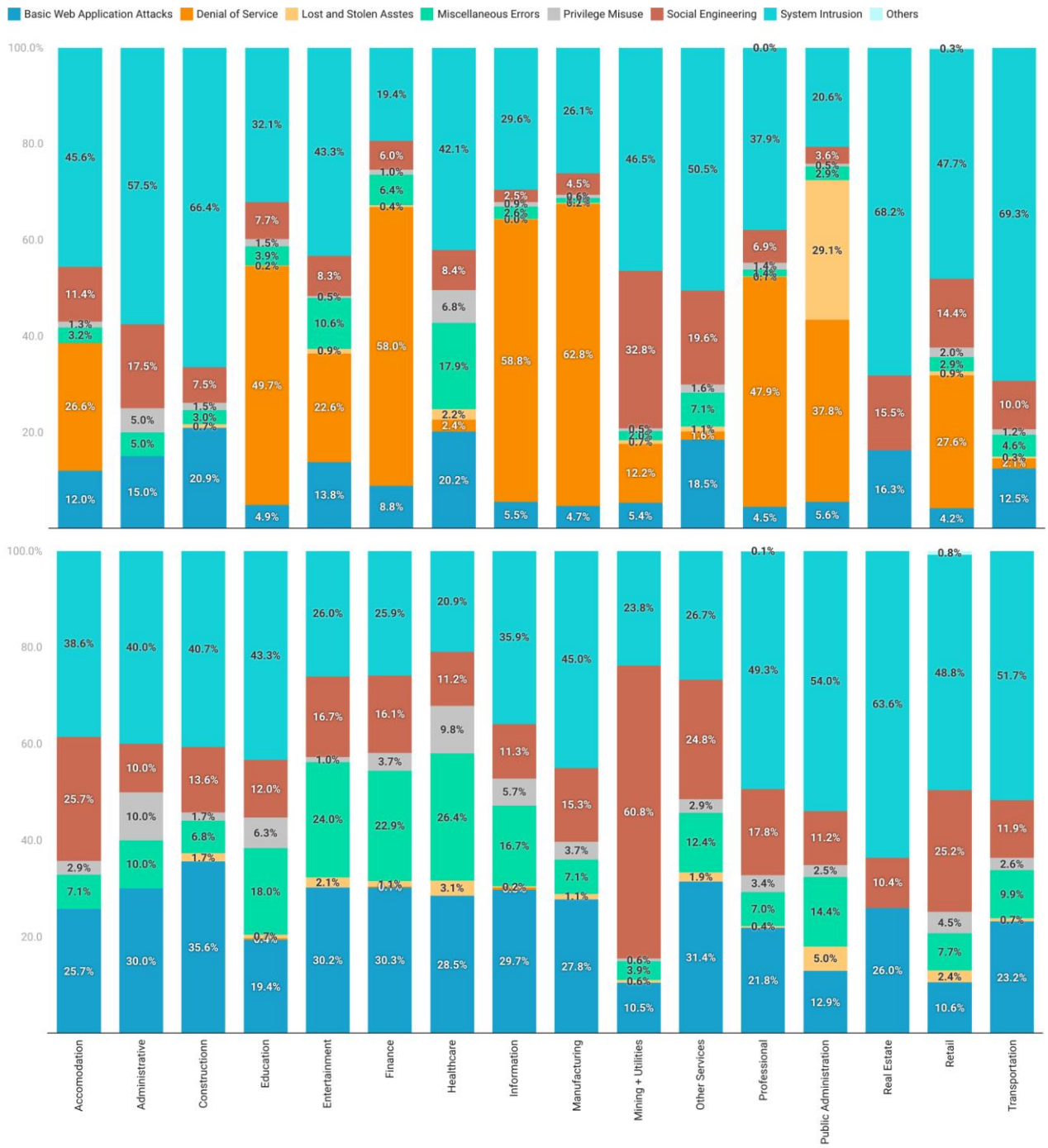


Fig. 3. Patterns of Cyber Incidents Fig. 4. Patterns of Cyber Breaches

Source: Advisen Data, Author's construction.

It is evident from Fig. 3 that basic web application attacks and system intrusions are the top patterns, accounting for 60% to 90% of the cyber-related incidents and breaches across all

industries. Financial institutions are no different except the comparatively higher percentage of miscellaneous errors, commonly as misdelivery of sensitive information to wrong clients, which has been on the rise over the years. A report by the Data Breach Investigations Report 2022 states that they estimate misdelivery to be approximately three times higher in the financial institution vertical than in other industries.[24] The study also boils down system intrusion to two main factors ransomware and DoS attacks; in the finance industry, personal data is compromised approximately three times as often as banking information.[25] The finance industry ranks fourth in terms of the number of the cyber attacks (2007-2022 Q2; *data source*)[26], and continues to be affected by financially (10.57% of incidents and 13.23% of breaches related to cyber security across industries) motivated organised crime, typically via phishing, hacking, and malware attacks.

5.4 Cross-Country Analysis

This section examines the world's regions in accordance with the United Nations M49 standards[4], and the data on the incidents and breaches used (Fig. 7) in the study comes from the following regions:

[24] Mansfield-Devine S, *Verizon: Data Breach Investigations Report*, (2022) https://www.verizon.com/business/resources/reports/dbir/.
[25] Id.
[26] *supra* at 24.

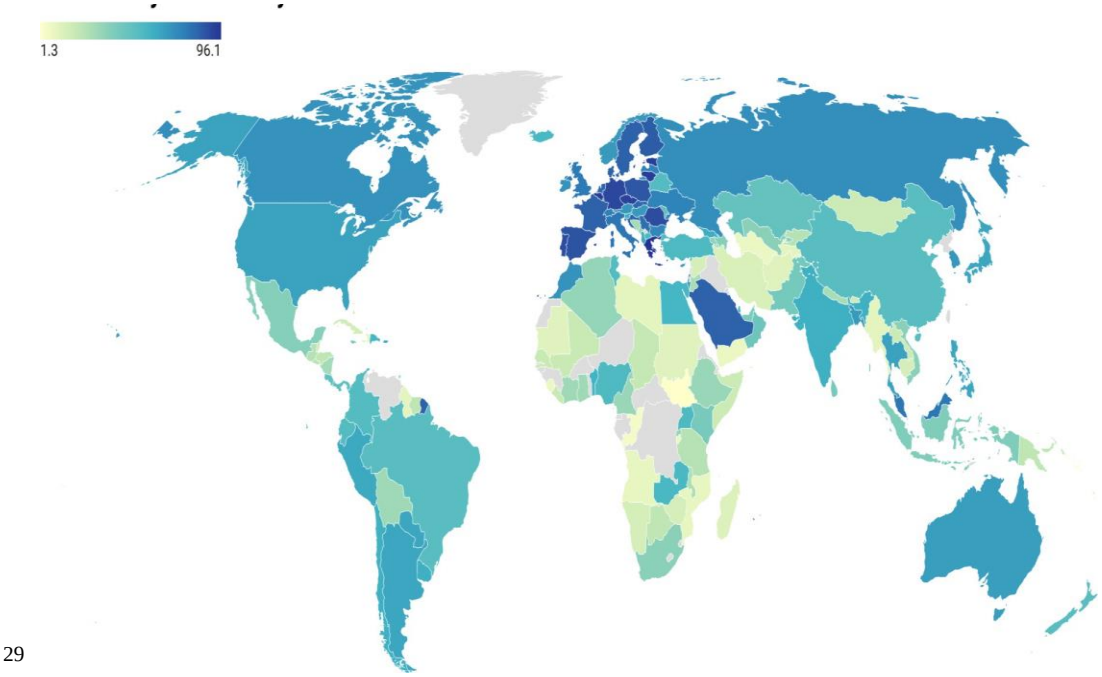
Table 1. World's Regions (United Nations M49 standards)

World Region	Countries
Asia and the Pacific **(APAC)**	Southern Asia, South-Eastern Asia, Central Asia, Eastern Asia, and Oceania
Europe, Middle East and Africa (**EMEA)**	North Africa, Europe and Northern Asia and Western Asia
Latin America and Caribbean (**LAC**)	South America, Central America and Caribbean
Northern America (**NA)**	Majorly United States and Canada

Table 1: World's Regions (United Nations M49 Standards)[27]

The map below (Fig. 5) demonstrates the variation in cybersecurity practices among nations, plotted with a global live index, the National Cyber Security Index, which measures countries' cyber security capacities that are implemented by their central governments. In other words, it measures the preparedness of countries to prevent cyber threats and manage cyber incidents.[28] The index is based on a variety of indicators: cyber security policy, education, and professional development; protection of digital and essential services; personal data; e-identification and trust services; cyber incident response; and cyber crisis management.

[27]United Nations Statistics Division, *Methodology: Standard country or Area codes for area codes (M49)*, https://unstats.un.org/unsd/methodology/m49/
[28] National Cyber Security Index, https://ncsi.ega.ee/methodology/ (last visited Mar 10, 2024).



29

Fig. 5. National Cyber Security Index.[30]

From the above map of the world, it is evident that the NCSI is highest in the western part of Europe, where Spain, the Czech Republic, France, Portugal, Poland, Belgium, and many other countries have NCSI values of more than 85. Accompanying these countries are French Guiana, which is located on the northeastern coast of South America; Saudi Arabia in western Asia; and Malaysia in southeastern Asia. On the other hand, a major part of Northern Europe and Northern America have the index values slightly above the median, while the countries below the median include most parts of northern and southern Africa along with some parts of Asia: Mongolia in eastern Asia; Myanmar, Laos, and Cambodia in south-eastern Asia; and Turkmenistan, Tajikistan, Afghanistan, and Iran in southern Asia.

Even though NCSI is a descriptive indicator of a country's cyber security development, it does not present a complete picture. A limitation to this measure is that it fails to account for the development of the IT infrastructure of a country, which plays a significant role in the scale and sophistication of cyber attacks. Thus, we calculate a development index for each country based on

[29] *Id.*
[30] National Cyber Security Interest, https://ncsi.ega.ee/ncsi-index/

the ICT Development Index[5] and Networked Readiness Index[6] indices.

$$\text{Development Index} = \left(\frac{NRI + IDI}{2}\right) \times 100$$

The difference between NCSI and the development index presents evidence of a country's cyber security development in accordance with its IT infrastructure development. The below map is plotted with the difference of the two indices, and the analysis differs vividly. Countries in the western Europe still presents more development in cyber security area than than its digital counterpart. On the other hand, the parts of northern and southern Africa, which were earlier on the lower end of the range of NCSI, show a positive measure when
digital development is considered. Moreover, India, Pakistan, and Bangladesh also depict that their cyber security is way ahead of the country's IT development. Libya in North Africa; Iran and Mongolia in Asia; Suriname and Guyana in South America remain on the lower range of the index, indicating poor cyber development.

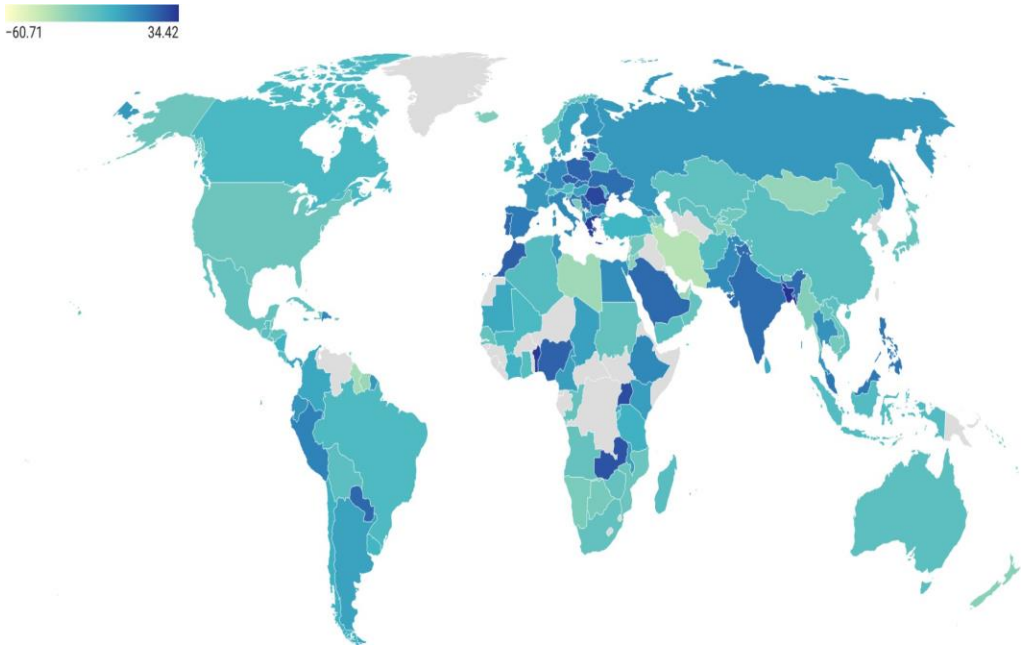


Fig. 6. Development Index.

Source: Author's construction[31].

[31] *Id.*

5.5 Identifying Patterns of Cyber Attacks

Our analysis of the Advisen data revealed some patterns in cyber security incidents and breaches, which are depicted in the charts below.

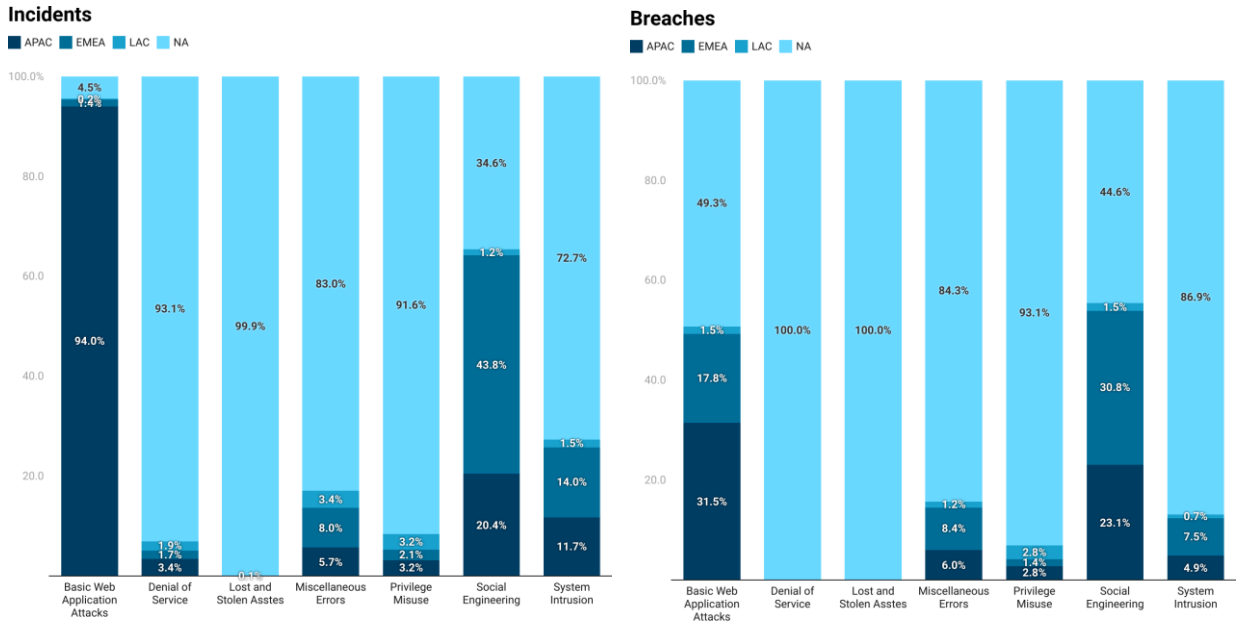


Fig. 7. Patterns of Cyber Incidents and Breaches (Cross-UN Regions).

Source: Advisen data, Author's construction.

There are relatively fewer countries in Asia with no proper records of cyberattacks than in Africa and Northern America. It is quite evident that APAC and EMEA mostly face basic web application attacks along with social engineering and system intrusions, while LAC suffers from miscellaneous errors that primarily take place in the finance industry. Even though around 94% of the basic web application attack incidents happen in the APAC region, rarely do they convert into a cyber security breach (<30%). An important point to note here is that even though Northern America has a good NSCI, it faces the highest number of cyber-related incidents and breaches. This indicates a very high bias in the database, which is due to robust breach disclosure laws in North America and better record coverage in the region. Further, a report by the DBIR team mentions that around 90% of the cyber attacks have a financial motive, which leads us to find a quantitative measure for the cyber risk involved in the banking industry across countries.

5.6 Risk Insurance

From the earlier sections, there is no denying that cybercrime is on the rise and financial institutions are frequently targeted by cybercriminals. According to an article published by the Mercator Advisory Group, ransomware attacks on the banking industry increased by 1,382% year-over-year in the first half of 2021.[32] Cybercriminals view banks as lucrative because they can earn money through a variety of methods, such as the sale of customer data, the theft of credit card numbers, and the commission of fraud. According to IBM's 2022 Cost of a Data Breach report,[33] the financial sector has the second highest average total cost of a data breach in 2022, averaging $5.97 million (much more than the average cost of other industries, and thus the report includes the financial services vertical under critical infrastructure organizations). It also finds that about 28% of the financial firms experienced a destructive or ransomware attack, while 17% experienced a breach because of a business partner being compromised.[34] Thus, these institutions also tend to employ increasingly sophisticated security measures to safeguard their high-value assets in response. However, there is another aspect to eliminating the risk: the question for institutions is not "if" they will be victimized by cybercrime, but "when".[35] Immediately following a data breach, businesses often find themselves in a flurry of activity as they try to assess the situation, determine what information was compromised, identify who gained access to it, determine if any individuals are at risk, and take corrective measures as soon as possible. In a situation that is already stressful, organizations must be ready to fulfill their legal responsibilities to victim clients and the regulatory bodies, which can be challenging. This can be systematically handled when the businesses are cyber-risk insured. In the event of a data breach involving sensitive information or a disruption to an organization's secured network, cyber insurance can help cover the costs associated with repairing the damage and restoring service. Although it does not prevent a hack itself, it does provide assistance before, during, and after one.[36] Insurers can assist businesses in assessing their

[32] Kimberly Johnson, *The Impact of Cyber Insurance on the Financial Sector*, PAYMENTS JOURNAL (Mar 11, 2024, 11:24 AM), https://www.paymentsjournal.com/the-impact-of-cyber-insurance-on-the-financial-sector/ [hereinafter "Kimberly"]
[33] IBM, https://www.ibm.com/downloads/cas/3R8N1DZJ (last visited Mar. 11, 2024).
[34] *Id.*
[35] Tyler Anders, *The Ever Increasing Threat of a Data Breach in 2021*, JD SUPRA (Mar 11, 2024, 11:22 AM) https://www.jdsupra.com/legalnews/not-if-but-when-the-ever-increasing-8569092/
[36] Kimberley, *supra* note 30

current risk profile. As a result of the unprecedented increase in risk since the pandemic's start, cyber premiums increased by more than 25 percent in Q2 of 2021.

Even though insurance has helped reduce the financial impact of cyberattacks, it has also led to questions and disagreements between financial institutions and their insurers when an attack leads to multiple types of losses. The majority of the world's insurance markets cover businesses, their assets, and their legal obligations. Unfortunately, cyber risk is not typically covered by insurance policies because they focus instead on protecting physical assets. Moreover, the relevance of cyber incidents to the terms of a contract may also be unclear. Since

the judge's decision and legal fees are clouded by this uncertainty, insurers face a greater financial risk. Accordingly, insurance companies work to clarify the terms of contracts in two ways. The insurer may revise its coverage either by explicitly excluding such risks from its standard policies and instead offering new, stand-alone policies or by including such risks and charging higher premiums. The American market is significantly more developed than its equivalent on the European continent. This is largely attributable to the fact that, for a number of years, the United States has enforced stringent disclosure rules for cyber attacks and that those who violate these rules face stiff consequences. When it comes to insurability challenges with cyber risk, Biener et al. (2015) identify three significant points. Firstly, there is no guarantee that losses will be independent and predictable, so risk pooling may not always be effective. Informational inequities are another major problem. In the wake of a devastating cyberattack, businesses are more likely to purchase insurance, leading to adverse selection as a result of the heightened competition among insurers.[37] Insurers mitigate the negative effects of selection via screening methods like upfront audits, underwriting questionnaires, and signaling. Lastly, there is the possibility of moral hazard, which occurs when policyholders alter their behavior as a result of having insurance.[38]

Given the policy's lengthy exclusions and the ever-changing nature of internet hazards, the actual coverage provided by the insurance plan is not quite apparent. Furthermore, there is no industry-wide terminology for insurance, making it a herculean task to compare different insurance policies. The insurance market has already begun seeing entrants that aim at collecting data. With an increased capacity and rise in the number of competitors in the insurance market, reduced

[37] Shackelford, S. J., *Should your firm invest in cyber risk insurance*?, 55(4) BUSINESS HORIZONS, 349-356, (2012).
[38] Eling, M., & Schnell, W, *What do we know about cyber risk and cyber risk insurance?,* THE JOURNAL OF RISK FINANCE 1526 (2016).

insurance rates are implicit. Moreover, this will lead to uniform market policies and product standardization. Conclusively, it is also crucial to focus on establishing industry-wide definitions and standards associated with cyber risk insurance.

6. FUTURE WORK

Due to the lack of a global quantitative assessment of cyber risk for the banking sector, we propose to construct a cybersecurity risk measure based on media coverage. The idea is to perform a textual analysis (similar to the one performed for the US) of verified newswires and articles that talk about cyber risks for each country. Furthermore, an approximate indirect measure can be calculated using the following approach:

$$\frac{Number\ of\ articles\ about\ cyber\ risk\ in\ financial\ sector}{Number\ of\ articles\ about\ cyber\ risk\ across\ all\ industries}$$

The aim is to formulate an industry-level cybersecurity risk index that is relative.

7. CONCLUSION AND POLICY RECOMMENDATION

Over the past five years, the number of cyberattacks has been increasing at an exponential pace, and specialists in the field of cybersecurity anticipate that by the year 2023, one incident will occur approximately every 11 seconds. Because of security lapses at numerous government organizations, credit bureaus, and large financial institutions, the personally identifiable information of a number of customers has become accessible to the general public. In the past, operational failures in the banking industry have been related to a wide variety of dangers. These risks include, but are not limited to, flaws in the system, fraudulent activity, legal action, and disruptions in the operations of the firm. As a result of a number of severe operational losses and a shifting capital structure, operational risk management has evolved as a discipline and become of the utmost importance. This is due to the fact that operational risk management has become of

the utmost importance. According to the findings of the Basel Committee, the Basel II accord outlines a total of seven possible approaches that might be taken in order to compute the operating risk capital charges. When compared to the sensitivities associated with business risk, the capacity of financial institutions to evaluate and assess cyber risk has not yet reached the level at which it can be consistently monitored. A textual analysis of the US-listed firms' disclosures and available Advisen data on cyber attack incidents were used in this research, with the end goal of developing a novel cybersecurity risk measure that can be applied to publicly traded companies in the United States.

Due to the sophisticated nature of today's cyberattacks, financial institutions must take precautions. Regardless of the fact that certain financial firms had formerly efficiently insured themselves with regard to cyberattacks, they are beginning to look to the commercial industry and the skills of analysts to aid them in better managing their risks.

To effectively disclose and address cyber-related dangers and occurrences, the following considerations should be taken care of by leaders and regulatory organizations:

Fig. 8. Recommendations for faster response to and recovery from cyber attacks, as well as better reporting of cybercrimes by the institutions.

Source: Author’s construction

The right corporate culture is just as important as using the relevant tool set when it comes to mitigating cyber risk and putting in place regulations that are necessary. This entails making the protection of sensitive data a priority in each and every department of the company. The development of a robust cybersecurity posture provides visibility into potential risks and assists in maintaining compliance with regulatory requirements.[39]

[39] IBM, https://www.ibm.com/in-en/industries/banking-financial-markets/cyber-security (last visited Mar. 11, 2024).