DEPARTMENT OF ACCOUNTING AND FINANCE

The influence of Financial Indicators and the impact of Cybersecurity policy on bank's performance.

MASTER THESIS

NEOFYTOS KOSTA

2024

University of Cyprus
Department of Accounting
and Finance

The influence of Financial Indicators and the impact of Cybersecurity policy on bank's performance.

Master Thesis in Finance

Neofytos Kosta

Supervisor: Andreas Charitou

Abstract

This study explores the relationship between bank cybersecurity policies and bankruptcy risk by integrating cybersecurity metrics with traditional financial indicators. Using data from 2013-2022, the research employs a mixed-methods approach to enhance the predictive accuracy of bank bankruptcy models. Logistic regression analysis reveals that banks with robust cybersecurity policies are approximately 2.8 times less likely to face bankruptcy compared to those without such policies. Additionally, a significant positive correlation between capital adequacy and the presence of cybersecurity measures highlights the financial resilience conferred by these practices. Despite these findings, the overall model fit is modest, indicating the need for further refinement to fully capture the interplay between cybersecurity and financial stability. The results suggest that integrating cybersecurity considerations into traditional financial health assessments can provide a more comprehensive understanding of bank resilience, offering valuable insights for bank executives, policymakers, and investors. This study contributes to the literature by emphasizing the critical role of cybersecurity in mitigating default risk and promoting financial stability, advocating for a holistic approach to financial risk management in the digital era.

Keywords: Bankruptcy Prediction, Cybersecurity Policies, Financial Indicators, Logistic Regression, Risk Management. CAMEL Model

Date: May 31, 2024

Πανεπιστήμιο Κύπρου

ΤΜΗΜΑ ΛΟΓΙΣΤΙΚΗΣ ΚΑΙ ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΗΣ

5 Ιουνίου 2024

Συντονιστή Μεταπτυχιακών Προγραμμάτων
Τμήματος Λογιστικής και Χρηματοοικονομικής

ΒΕΒΑΙΩΣΗ

Βεβαιούται ότι ο μεταπτυχιακός φοιτητής Νεόφυτος Κώστα (Αρ. Ταυτότητας 930266) ολοκλήρωσε με επιτυχία την προφορική υποστήριξη της διπλωματικής της μελέτης σε εξέταση που έλαβε χώραν ενώπιον διμελούς εξεταστικής επιτροπής, στις 27 Μαΐου 2024. Παρέδωσε την διπλωματική του μελέτη στις …………………………..

Η εξεταστική επιτροπή,

Ανδρέας Χαρίτου
(Πρόεδρος, Σύμβουλος)

Αδάμος Βλίττης
(Σύμβουλος)

Acknowledgements

I would like to express my deepest gratitude to my supervisor, Professor Andreas Charitou, for his invaluable guidance, support, and encouragement throughout this research. His insightful feedback and unwavering patience have been instrumental in the completion of this study.

I also extend my sincere thanks to the University of Cyprus, particularly Mr. Marios Kyriakou, for providing access to essential data and resources that were crucial for this research.

A special thank you to my family and friends for their continuous support and understanding during this journey. Your belief in me has been a source of great motivation.

Finally, I am grateful to all the participants and institutions that contributed to this study. Your cooperation and assistance have made this research possible.

Thank you all.

Table of Contents

1 Introduction

Examining the correlation between banks implementing cybersecurity policies and their bankruptcy risk is crucial for several reasons. With frequent cyber-attacks targeting banks' sensitive data, understanding if these policies effectively reduce risks is vital. Research can show whether such measures help prevent cyber-attacks and data breaches, lowering the chance of bankruptcy. This insight can guide policymakers and banks in adopting effective risk management practices. Ultimately, understanding the link between cybersecurity and bankruptcy risk can strengthen the financial sector, protecting it from systemic threats posed by cyber-attacks.

Several motivations drive the study examining the relationship between banks' cybersecurity policies and their bankruptcy risk. As cyber-attacks on financial institutions rise in both frequency and complexity, it's crucial to determine if cybersecurity investments effectively lower default risk. Banks must allocate resources wisely for risk management amid stricter regulatory demands. Weaknesses in cybersecurity frameworks could propagate systemic risks across the global financial system, emphasizing the need for thorough research to enhance resilience and mitigate such threats. Ultimately, the study's motivation lies in promoting the resilience of financial institutions and safeguarding the integrity of the banking sector in an increasingly digitized world.

The main issue in this research study is to seek to establish the effect of cybersecurity on the financial health of banks, emphasizing mainly its ability to predict bank bankruptcies. This argument arises out of a more acute concern over cyber threats and their potential to disrupt financial stability (Schinasi & Teixeira, 2006). Within this context, it's essential to question if traditional financial indicators suffice to diagnose a bank's health amidst evolving cyber threats. This study aims to merge cybersecurity metrics with conventional financial indicators for a more comprehensive assessment of bankruptcy risk.

Considering this, the objectives of this research are multi-dimensional. First, it seeks to identify key financial indicators that in the past predicted bank failures such as total equity/total assets and NIM (Demirgüç-Kunt, Detragiache, & Merrouche, 2013). Secondly, it seeks to establish how measures with using policy on cybersecurity in place to protect from cyber-attack, unauthorized access, and data leaks are correlated to these financial indicators. This aspect builds on the work by Romanosky (2016) that quantifies the cost of cyber incidents and hence presents a framework through which these costs may be integrated into financial assessments.

Another goal is to use a mixed-methods approach, blending qualitative cybersecurity assessments with quantitative financial data to create a regression model for more accurate bank bankruptcy predictions. This method is in line with the recommendation by Hosmer, Lemeshow, & Sturdivant (2013) that will be used to analyze dichotomous outcomes such as bankruptcy. It is, therefore, the objective of this study to provide a new model that integrates the cybersecurity factor in financial health assessments and enhance the knowledge in the subject towards addressing that gap identified in the literature by Gatzlaff & McCullough (2010) regarding classic financial models ignoring digital vulnerabilities.

This study extends the existing literature in several keyways. Firstly, it contributes to the growing body of research on the intersection of cybersecurity and financial risk management by specifically focusing on banks' default probability. While previous studies have explored the impact of cybersecurity on various aspects of financial institutions, such as operational efficiency and reputation risk, this study provides novel insights into its direct influence on default risk. By filling this gap, it enriches our understanding of the broader implications of cybersecurity practices in the banking sector.

Furthermore, this study may uncover nuanced relationships between specific cybersecurity measures and default probability, offering practical implications for bank management and policymakers. By identifying which aspects of cybersecurity most effectively mitigate default risk, it can inform strategic decision-making regarding resource allocation, investment priorities, and regulatory compliance**.** Additionally, by considering the dynamic nature of cybersecurity threats and regulatory landscapes, this study may highlight evolving challenges and opportunities for the banking sector. It can serve as a foundation for future research endeavours exploring emerging trends, innovative technologies, and evolving best practices in cybersecurity and financial risk management.

This study deepens our understanding of the complex link between cybersecurity and default risk in banking, enriching discussions on cybersecurity resilience and financial stability. By integrating cybersecurity metrics into the CAMEL model, it offers a more comprehensive approach to assessing bank health in the digital era. This timely integration addresses escalating cyber threats, aiding in a more precise grasp of financial stability in banking. Examining the correlation between banks' cybersecurity policies and default probability is vital to various stakeholders. It informs bank executives and risk managers on strategic resource allocation, risk mitigation, and compliance strategies.

Regulators and policymakers are also interested in this research due to the escalating cyber-attacks on financial institutions. They aim to ensure the banking sector's resilience and can use insights from this study to shape regulations on cybersecurity standards, risk management, and reporting. Additionally, investors and shareholders are affected by cybersecurity incidents, which can lead to reputational damage, legal issues, and financial losses for banks. Hence, they rely on risk assessments, including cybersecurity, to make investment decisions and gauge the stability of financial institutions.

Moreover, customers and the public are also affected by the outcomes of this research. A bank's ability to protect sensitive financial and personal information from cyber threats directly impacts customer trust and confidence. By understanding the effectiveness of cybersecurity measures in reducing default risk, customers can make more informed choices about where to entrust their financial assets and personal data. The investigation of this topic is important to a wide range of stakeholders as it directly relates to financial stability, regulatory compliance, investor confidence, and consumer trust in the banking sector. By shedding light on the relationship between cybersecurity and default risk, this research contributes to the resilience and integrity of the financial system.

With this study, we contend that there exists a significant relationship between the implementation of cybersecurity policies in banks and their default probability. By rigorously analysing data and examining the effectiveness of various cybersecurity measures, we aim to provide empirical evidence supporting this assertion. Furthermore, we contend that understanding this relationship is essential for informing strategic decision-making by bank executives, guiding regulatory initiatives, assisting investors in assessing risk, and bolstering consumer trust in the banking sector. Ultimately, our findings contribute to enhancing the resilience of financial institutions against cyber threats and promoting overall financial stability.

The justification and relevance of this study are based on the emerging landscape of financial risk management with a focus on the banking sector. These phenomena together with the rising incidence of cyber threats and their potential to disrupt financial stability are well documented phenomena, which call for reassessment of conventional risk models (Biener, Eling, Wirfs et al., 2015). The focus of this study integrating cybersecurity metrics to the classic financial indicators for the bank bankruptcy isn’t only timely but indispensable in this era that digital threats can reach long down the road the banks.

Another factor that makes this study relevant is the emerging recognition of cyber risk as among the significant impacts to the financial industry. The Basel Committee on Banking Supervision (2018) identifies cyber risk as one of the major types of operational risk exposures faced by banks, pointing towards a need in frameworks for an improvement of assessment of and response to this threat. Such a recognition is in line with the objectives of this research to incorporate cyber risk metrics in the bankruptcy prediction models. In addition, Romanosky (2016) goes on to point that cyber incidents have a quantifiable financial impact hence there is a rationale for their inclusion as key factors in the assessment of bank's financial health.

In the European banking sector, there's a unique context with varying regulatory environments, while cyber threats are transnational. The European Central Bank (2019) emphasizes the importance of cybersecurity for financial institutions, reflecting the seriousness with which these challenges are addressed. This study focuses on European banks, providing region-specific yet globally relevant insights. It responds to the need to adapt financial risk assessment models by including cyber risk as a crucial factor for banks' stability. Regulators increasingly prioritize cyber risk alongside ongoing digitalization in the financial sector. This research aims to bridge the gap between traditional financial risk assessment metrics and cyber risk metrics, benefiting academic literature and practical risk management in banking.

This paper uses a sample dataset that includes various financial indicators and cybersecurity metrics for the period 2013-2022. The sources of data have been chosen from the S&P Market Intelligence Platform and from data collected from the UCY databases after communication with the relevant department and the professor in charge Mr. Marios Kyriakou due to their comprehensiveness and richness for capturing the dynamism of cyber threats and implications on the performance of banks (S&P Global Market Intelligence, 2021). These variables have been well-recognized in financial analysis literature and are very essential to understand about the firm's financial health and risk of bankruptcy (Wooldridge, 2015). These variables create the CAMEL approach which helps to predict the financial stability of financial organizations. Shapiro-Wilk's test was used to test the normal distribution of these variables in the analysis to ensure that subsequent statistical analyses were appropriate (Shapiro & Wilk, 1965).

Furthermore, the study utilizes logistic regression analysis which is methodically sound in evaluating the prospect of binary outcomes as in bankruptcy cases (Hosmer, Lemeshow, & Sturdivant, 2013).This approach allows for a deeper examination of the relationship between traditional financial indicators and the emerging factor of cybersecurity, enhancing understanding of contemporary bankruptcy risks. The methodology is characterized by quantitative rigor and innovative integration of cybersecurity factors into financial analysis. It aligns with modern financial research paradigms and contributes to the evolving field of assessing financial risk in the digital age.

Study findings, with first tested the paired sample, not revealing a statistically significant relationship between cybersecurity metrics and bankruptcy risk. On the other hand, results uncover intriguing correlations that contribute significantly to the extant literature. The observation that the ratio of Capital Adequacy is higher in organizations with a cybersecurity policy compared to those without highlights the potential synergies between cybersecurity measures and financial resilience. These finding challenges conventional assumptions and suggests that institutions prioritizing cybersecurity may also demonstrate stronger capital adequacy, which is crucial for withstanding financial shocks and reducing default risk. This insight adds depth to discussions about broader benefits of cybersecurity investment beyond mitigating cyber threats alone.

Secondly, the identified correlations between Management ratio and Capital Adequacy, as well as Earnings ratio and Capital Adequacy, provide valuable insights into the interplay between classic banking metrics and financial stability in the context of cybersecurity. These correlations suggest potential pathways through which management effectiveness and earnings performance may influence capital adequacy levels, thereby indirectly affecting default probability. Understanding these relationships can inform more holistic risk management strategies.

After testing all the available sample found that the presence of cybersecurity policies significantly reduces the likelihood of bank default, with banks lacking such policies being approximately 2.8 times more likely to default. This underscores the crucial role of robust cybersecurity measures in mitigating default risk, suggesting that banks should prioritize developing and implementing comprehensive cybersecurity strategies. The highly significant positive relationship between cybersecurity and default probability emphasizes the need for stringent regulatory standards to ensure banks' cybersecurity readiness.

Additionally, the analysis reveals that capital adequacy has a significant negative relationship with default probability, indicating that higher capital adequacy drastically lowers the odds of default. This finding supports the importance of maintaining strong capital reserves as a buffer against financial instability. In contrast, variables such as asset quality, management, earnings, and liquidity were not found to have significant impacts on default probability. These results provide valuable insights for policymakers and bank managers, highlighting the importance of cybersecurity and capital adequacy in maintaining financial stability and reducing default risk.

Moreover, this study contributes methodologically by demonstrating the importance of examining indirect effects and exploring alternative pathways when investigating complex phenomena like cybersecurity's impact on default probability. By uncovering unexpected correlations and highlighting nuanced relationships, this research encourages scholars to adopt a more comprehensive approach to analyzing the multifaceted dynamics of cybersecurity in the banking sector.

This research highlights the importance of integrating cybersecurity metrics into financial health assessments, aligning with recent studies emphasizing the financial impact of cyber risks (Romanosky, 2016). Beyond academic contributions, this integration offers practical insights for financiers and regulators, urging a re-evaluation of risk assessment models in banking to include cyber risk, as advocated by the Basel Committee on Banking Supervision (2018). Overall, the study enriches existing literature by providing new insights into the relationship between cybersecurity, traditional banking metrics, and default risk. By elucidating these complex connections, it advances discussions on cybersecurity's broader implications for financial stability and risk management, facilitating more informed decision-making in academia and industry.

The rest of the paper is organized as follows: Section 2 provides the Institutional/Theoretical/Regulatory Framework. Section 3 describes our research design, while sample construction and descriptive statistics are presented in Section 4. Sections 5 presents the empirical results and Section 6 concludes.

2 Theoretical/Regulatory Framework

2.1 Theoretical Background

The theoretical framework of this study revolves around the intersection of financial risk management and information security, a convergence gaining prominence as cyber threats escalate in today's business landscape. Drawing on established theoretical paradigms such as Modern Portfolio Theory (MPT) and the Efficient Market Hypothesis (EMH), alongside theories of corporate governance and information asymmetry, the research seeks to elucidate the relationship between cybersecurity and bankruptcy prediction.

Modern Portfolio Theory, first advanced by Harry Markowitz in 1952, traditionally focused on optimizing investment portfolios based on market risks and returns. However, in the context of cybersecurity, MPT principles are increasingly applied to diversifying investments in cybersecurity measures, aiming to mitigate overall financial risk associated with cyber threats.

One of the leading finance theories existing to date is the Efficient Market Hypothesis authored by Eugene Fama in 1970, purporting that "financial markets are informationally efficient where securities prices at any time fully reflect all available information" (Fama, 1970). Incorporating cybersecurity information challenges EMH, suggesting that market valuation and financial stability may be influenced by perceptions of a company's cyber resilience or vulnerability, impacting bankruptcy prediction.

Another relevant theoretical framework is the information asymmetry theories, specifically Akerlof’s "Market for Lemons" (1970) that highlight the potential for misjudged decisions due to stakeholders' lack of precise information about a firm's cybersecurity risks or policies. This aligns with the study's finding that organizations with cybersecurity policies tend to exhibit higher Total Equity/Total Assets ratios, implying favorable market perceptions of security.

In addition, theories supporting cyber risk management measures such as the Gordon-Loeb Model have been handy in explaining the appropriate investment in cybersecurity measures (Gordon & Loeb, 2002). This theoretical perspective supports the study's analysis of cybersecurity metrics and their integration with classic financial indicators in bankruptcy prediction models.

Furthermore, the consideration of systemic risk factors, as discussed by De Bandt and Hartmann 2000, underscores the broader implications of cybersecurity risks on financial sector stability. This study extends this discussion by examining how cybersecurity risks contribute to systemic risk within the banking sector, highlighting the need for comprehensive risk management strategies.

In conclusion, the theoretical background of this study is confluence between traditional theories relating to financial risk management and emerging perspectives in cybersecurity risk management. This amalgamation demands essential understanding and prediction of the financial stability of organizations in an increasingly digitalized world, where cyber threats pose significant risks alongside classic financial factors.

2.2 Regulatory and Institutional Context

The study's regulatory and institutional context is important within which the continuously changing dynamics charactering financial risk management as well as cybersecurity in the banking sector needs to be understood. This context is set by international regulations, national legislative framework, and institutional policies which all aim at minimizing financial risks including those that are emerging from cyber threats.

The Basel Committee on Banking Supervision (BCBS) leads international efforts in regulation and has basically set the guidelines for bank regulation. Through the BCBS's loss data collection exercise, the industry was able to quantify its operational risk exposure and, at long last, the BCBS has given broader accepted recognition to cybersecurity as a component of operational risk. In their paper "Basel III: The Net Stable Funding Ratio" (2010), the committee stressed that stability in funding and liquidity require to be supported even under the influence of cyber risks. Additionally, the BCBS guidance on cyber resilience (2018) makes it clear that banks have to focus on building strong frameworks of the identification, protection against, detection, response to, and recovery from cyber-attacks.

The European Union (EU) has similarly played a significant role in shaping the regulatory environment. For example, with the effective date of 2018, the General Data Protection Regulation (GDPR) sets stringent data protection conditions for all operations within the EU and thus has a great impact on cybersecurity management in banks (Voigt & Von dem Bussche, 2017). Another key piece of legislation, the EU's Network and Information Systems (NIS) Directive is looking for appropriate security measures in place asking critical sectors like banking to manage cyber risks.

At the national level, those countries within the EU have transposed these directives through their legislations while varying its nature to suit their context. For example, Germany's Federal Office for Information Security (BSI) is an essential organ that supervises and guides on the matters of cybersecurity in the financial sector while reflecting on the EU-wide directives that still remain aware of national situations (Gerlach, 2019).

Financial sector cybersecurity risk is guided by the Federal Financial Institutions Examination Council (FFIEC) of the United States. Their well-known Cybersecurity Assessment Tool (CAT), as they put it, helps identify such risks and their measurable impact on an institution or a financial organization as well its preparedness to handle them (FFIEC, 2017).

It is important to consider the place of institutional policies in shaping practices of cybersecurity within banks too. Institutional policies are, in turn, often shaped on the basis of both sets of the external prescription as well as internal risk assessments. For instance, some of these frameworks include ISO/IEC 27001, a major information security management international standard, which has increasingly found usage for several banks in order to enhance their status against cybersecurity (Calder & Watkins, 2012).

Underpinning these regulatory and institutional frameworks is a theoretical understanding based on the concept of minimizing systemic risk as central in ensuring financial stability. It is worth noting that a cyber attack on a singular institution can trigger cascading effects on the whole financial system as observed by De Bandt and Hartmann (2000). Consequently, focusing on strong requirements of cyber-security is not merely meant to protect individual institutions but also that of the entire financial ecosystem.

Additionally, the invasion of financial technology (FinTech) companies has added dimensions to the regulatory environment. Usually being less regulated than traditional banks, FinTech companies pose competitive threats while possibly posing cybersecurity risks by the mere fact that they are in controlled possession of large amounts of sensitive financial data (Arner, Barberis, & Buckley, 2016).

In conclusion, the regulatory and institutional context represented in this study mirror a multifaceted approach managing financial and cyber-security risks within a banking context. This approach includes a complex interaction of international standards, national legislations, and institutional policies all targeted at ensuring the cyber resilience of the finance system.

3. Literature Review, Motivation, Hypotheses, and Expectations

3.1 Literature Review

The current bankruptcy prediction literature has always focused primarily on financial metrics and an increasing emphasis is given to the application of novel factors like, for instance, cybersecurity. The present work aims to provide this context within the greater field in the following short literature review.

An empirical study about default of banks is the study of Charitou(2015) who examined if the new measures for performance suggested by the Basel Accord on Banking Supervision are important in explaining bank default and weather if the new model with the three new variables has better accuracy in prediction compared to the existing one and he found statistically significant those variables. The author found results that support Basel's Committee decision to place additional restrictions on banks on capital adequacy, liquidity and earnings. His main hypotheses were if the three suggested performance measures included in the CAMELS Model are more important in explaining bank default compared to the previous measures and if the new CAMELS Model has greater prediction accuracy compared to the previous CAMELS Model. The author split the sample into training and testing and by using the variables of the CAMELS Model, he made the predictions in order to see if the prediction is correct. The condition of the prediction is that if the probability of default of the healthy bank is less than 50% and the probability of default of a bankrupt bank is more than 50% then the prediction is correct. According to the author, that study differs from other studies because nobody tests the three new variables suggested by the Basel Committee and also the overall prediction of the model is very high, and the Type I error is very low compare to most of other studies. Integrating cybersecurity into a predictive model of bank failure based on the CAMEL framework would likely enhance the model's ability to anticipate and mitigate risks to financial institutions, aligning with the evolving landscape of cybersecurity threats in the banking sector.

Jordan et al. (2010) conducted a study comparing failed banks with non-failed banks from 2007 to 2010, focusing on the market-to-book ratio. Their findings indicate that a formula incorporating seven specific variables can predict bank failure with varying levels of accuracy, ranging from 66.0% to 88.2% over one to four years. These variables demonstrate significant explanatory power concerning the market-to-book ratio. The primary hypotheses of the study are: 1) the identified seven variables can predict bank failure up to four years in advance, 2) the ratio of expense provision for bad debts as a percentage of total gross loans serves as a predictor of bank failure, and 3) the ratio of real estate loans as a percentage of total assets acts as a predictor of bank failure. Consistent with expectations, higher levels of non-accrual and real estate-owned assets, as well as increased real estate loans, correlate with elevated rates of bank failures, while higher Tier One capital ratios are associated with fewer failures. The study's overall regression model yields statistically significant results. Additionally, the authors employed a sample split into training and testing groups to develop and validate a discriminant function. The outcomes reveal successful predictions ranging from 66.0% to 88.2% of failed banks, with an overall success rate of 76.8%. Hypotheses 1 and 3 are supported by the overall models, while hypothesis 2 remains inconclusive. Incorporating cybersecurity as an additional variable into the predictive model could enhance its accuracy by considering the impact of cyber threats and vulnerabilities on a bank's overall risk profile. Just as Jordan et al. examined different variables to predict bank failure, including cybersecurity alongside the CAMEL framework could provide a more comprehensive understanding of the factors influencing a bank's likelihood of failure.

In the late 20th and early 21st centuries, researchers such as Ohlson (1980) and Shumway (2001) re-focused this with improved bankruptcy prediction models that incorporated market data and use of logistic regression techniques. This research can relate to predicting bank bankruptcy within the context of the CAMEL framework and incorporating cybersecurity considerations in several ways. Firstly, similar to analyzing financial ratios for firms, financial metrics within the CAMEL framework (Capital adequacy, Asset quality, Management quality, Earnings, and Liquidity) can be examined to assess the financial health and stability of banks. By evaluating these metrics, researchers can identify key indicators associated with bank failures and develop predictive models to forecast the probability of bank bankruptcy.e dynamic feature of the financial markets but still over anchored on classic financial indicators.

More recent studies have started to deepen into the influence of non-financial factors over financial health. For instance, Derrat et al. (2016) reviewed the effect of corporate governance over bankruptcy risk or Arena (2008), studied the macroeconomic conditions. In fact, such research studies typically illustrate the growing realization that the phenomenon of financial distress is Relating this to predicting bank bankruptcy within the CAMEL framework and incorporating cybersecurity considerations, corporate governance practices, including effective risk management and transparent decision-making, influence management quality, capital adequacy, and earnings components of the CAMEL framework. Moreover, integrating cybersecurity factors alongside governance and the CAMEL framework provides a comprehensive approach to predicting bank bankruptcy, considering the evolving digital banking landscape's risks. By incorporating these insights, researchers can develop more models for predicting bank bankruptcy and identifying effective risk management strategies.multidimensional and also affected by a greater variety of factors than has traditionally been accepted.

Shifting attention to the world of cybersecurity, scholars have initiated measuring the financial impact of cyber incidents. Costs of cyber breaches are analyzed by Romanosky (2016) and he says that they have major bearing on the financials of companies. Gordon and Loeb (2002) carry it further to conduct an analysis into the economics of cybersecurity investments, indicating guidelines in regard to settling for an optimal level of spending which companies can follow to ensure risk-management is explicable. The studies by Romanosky (2016) and Gordon & Loeb (2002) offer valuable insights into the economic aspects of cybersecurity incidents and investment in information security, respectively, which can be related to CAMEL and cybersecurity bank bankruptcy prediction. Romanosky's examination of the costs and causes of cyber incidents sheds light on the financial implications of cybersecurity breaches, highlighting the importance of assessing risks related to cyber threats within the CAMEL framework. Understanding the economic impact of cyber incidents can inform banks' risk management strategies and investment decisions, particularly in bolstering cybersecurity measures to mitigate potential threats to financial stability. Similarly, Gordon and Loeb's research on the economics of information security investment provides a framework for evaluating the cost-effectiveness of cybersecurity investments, which can be integrated into the risk assessment process within the CAMEL framework. By considering the economic rationale behind cybersecurity investment decisions and aligning them with the risk factors outlined in the CAMEL framework, banks can enhance their ability to predict and prevent cybersecurity-related bank bankruptcies.

Firstly, this study differs from the conventional approaches by virtue of incorporating cybersecurity metrics in the bankruptcy prediction model. Unlike existing models which are largely based on historical financial data and some market variables as the determinants, this time the model acknowledges the current threat landscape where cybersecurity risks are increasingly relevant. This is particularly considering the research of Eling and Schnell (2016) that emphasis the rising frequency and magnitude of cyber events in the financial sector.

Moreover, the incorporation of cybersecurity to the bankruptcy prediction models fills a gap realized in the literature. Although some studies have been done on the direct costs of cyber incidents, and others may have analyzed how these incidents impact classic financial risk metrics, they are rare or not available at all in the literature touching bankruptcy prediction. This research fills this research gap as this study would empirically investigate the way cyber security metrics interact with financial health indicators.

Therefore, to put it briefly, this study fills the literature gap where it intrinsically connects the traditional bankruptcy prediction models and cybersecurity. A shift from a purely financial perspective of risk to one more integrated, reflecting the complexities both of modern finance and the digital landscape. Doing so not only enhances the predictive power of conventional models but also offers more holistic understanding into the determinants of financial well-being in the present digital age.

3.2 Motivation of the Study

The motivation is drawn from changing dynamics of risk factors affecting financial stability in the banking sector more particularly through the inclusion of cyber risk as a major determinant. This has alerted the researchers to the fact that while classic financial indicators are very important, they may not be sufficient to represent the multi-faceted nature of bankruptcy risk by itself in this new digital age.

As a proof underlying importance of this research, it is possible to mention the growing prevalence and severity of cyber incidents within the financial industry. Romanosky (2016) has also conducted own study on that matter and demonstrated how much financial damages incidents similar to hackings may cause. All these cyber threats not only engage in immediate risk in operations, but also carry along long-term implications towards reputation and financial for the banks, hence a more comprehensive type of risk assessment should be done. This need is further discussed in the research by integrating cybersecurity metrics with the classic financial indicators, thus providing a more holistic perspective in the bankruptcy estimation.

Additionally, the regulation's focus on cyber risk management adds value to this research. Some examples that illustrate this regulatory push in recognizing and mitigating cyber risks in financial institutions include The Basel Committee on Banking Supervision (2018) and The European Union’s GDPR (Voigt & Von dem Bussche, 2017). This study, therefore, by aligning into these regulatory perspectives adds to the development of more risk assessment models attuned with the regulatory expectations as well as best practices.

Moreover, this study addresses an existing literature gap as the relations between cybersecurity and financial stability have remained poorly examined. With continued digitization of operations conducted by financial institutions, the brought together cyber risk and the financial health become a matter that calls for exceptionally extensive research. This study therefore provides invaluable insight on how cybersecurity measures would impact the financial indicators, hence allowing for even more subtle futuristic bankruptcy prediction models.

In summary, this study's significance is that it may improve the predictability of bankruptcy models with recent risk factors since these will be used to assess the risk in today's volatile digital atmosphere besides providing information for regulatory and strategic decisions in the financial industry.

3.3 Research Hypotheses

The grounding of the formulation of research hypotheses in this study is on the imperative to augment traditional bankruptcy prediction models with contemporary cybersecurity metrics. Integration of these metrics is hypothesized to enhance the predictive powers of these models, reflecting the increasingly digital landscape of financial operations, and associated cyber risks.

Hypothesis 1: The policy on cybersecurity in place to protect from cyber-attack, unauthorized access, and data leaks, negatively affect the bankruptcy risk. The hypothesis notes that forward investment in cybersecurity negatively correlates with the bankruptcy risk among banks. This hypothesis is based on the understanding that effective cybersecurity pays off as it has the ability to uniquely mitigate and limit in its own specific ways the operational and reputational risks emanating from cyber incidents such as to limit the damaging financial impacts.

Based on the literature review provided, several studies have examined the relationship between cybersecurity measures and financial stability within the banking sector. These studies offer valuable insights that can be used to support and extend Hypothesis 1, which states that the policy on cybersecurity affect negatively the bankruptcy risk. Romanosky (2016) study analyzes the financial impact of cyber incidents, emphasizing the significant damages that incidents like hacking can cause to financial institutions. This study highlights the importance of cybersecurity in protecting banks from potential financial losses associated with cyber threats. Building upon Romanosky's findings, this study can argue that a cybersecurity policy is essential for mitigating the financial risks posed by cyber incidents, indicative of a proactive approach to risk management. Banks with strong cybersecurity measures in place are better positioned to safeguard their financial health by mitigating potential losses from cyber incidents. Therefore, a comprehensive cybersecurity policy can serve as a predictive indicator of a bank's financial health, as it correlates with reduced bankruptcy risk, allowing banks to withstand and recover from cyberattacks more effectively.

Gordon and Loeb (2002) research delves into the economics of cybersecurity investments, providing guidance on optimizing spending to manage cyber risks effectively. Their analysis suggests that strategic investments in cybersecurity can yield significant cost savings by mitigating potential financial losses due to cyber incidents. By incorporating insights from Gordon and Loeb's study, this study can argue that investments in cybersecurity contribute significantly to maintaining financial health by protecting assets and ensuring operational continuity. Banks that allocate resources towards cybersecurity measures demonstrate a commitment to safeguarding their financial well-being, thereby predicting their overall financial health. A well-developed cybersecurity policy not only shields banks from financial losses but also enhances their overall financial stability. Efficient allocation of resources towards cybersecurity measures correlates with reduced bankruptcy risk, as banks proactively mitigate threats to their operations and reputation, reinforcing their resilience in the face of potential cyber incidents.

Also, Regulatory Perspectives (Basel Committee on Banking Supervision, GDPR) emphasize the importance of managing cyber risks in financial institutions. These regulations mandate banks to implement cybersecurity policies and practices to safeguard customer data and maintain operational resilience. Drawing on regulatory perspectives, adherence to cybersecurity regulations emerges as a crucial factor in reducing bankruptcy risk in banks. Compliance with regulatory standards signifies a commitment to maintaining a secure operating environment, which ultimately enhances financial stability and reduces the likelihood of bankruptcy. Banks that prioritize cybersecurity are more likely to have risk management practices in place, contributing to their overall financial stability. Therefore, compliance with cybersecurity regulations can be viewed as a predictor of financial health, as it reflects a proactive approach to risk management and regulatory compliance.

This hypothesis is predicated on the notion that if cybersecurity exposures were assessed and managed proactively, then a good picture of a bank's overall risk profile would emerge as opined by Böhme and Kataria (2006).

In summary, integrating insights from various studies supports the hypothesis that a cybersecurity policy significantly predicts and reduces bankruptcy risk within the banking sector. This underscores the critical role of proactive cybersecurity measures in enhancing financial stability and resilience against cyber threats. Such policies not only mitigate financial risks but also serve as predictive indicators of a bank's overall financial health. Institutions prioritizing cybersecurity are better positioned to manage risks associated with cyber threats, thus maintaining stronger financial positions. Consequently, incorporating cybersecurity considerations into financial health assessments can enrich predictive models, offering valuable insights into a bank's stability and resilience. This hypothesis aim to advance the contemporary understanding of bankruptcy prediction by integrating cybersecurity metrics, reflecting the evolving risk landscape in financial services where cyber-related risks are increasingly prominent alongside traditional financial risks. The study's hypothesis is crafted to assess the effectiveness of this integrated approach, potentially paving the way for more refined and up-to-date models of financial risk assessment.

4. Research Methodology

4.1 Dataset

This section presents the methodology followed for the construction of the Regression model in order to predict the bankruptcy of organizations. First, the time period of primary data collection, the data collection process, the sample of bankrupt companies, the sample of healthy companies and the method of statistical analysis of the collected data are described.

The integration of classic financial indicators and the newly recognized impairment because of cyberattacks calls for a refined approach in predicting bank bankruptcies. This study used a mixed-methods design that converges both qualitative and quantitative results to allow for the most holistic reading of the findings.

The primary dataset contains financial indicators and cybersecurity metrics from covering a temporal extent of ten years. Dataset drawn from the S&P Market Intelligence Platform for the CAMEL variables and from data for cybersecurity variable collected from the UCY databases after communication with the relevant department and the professor in charge Mr. Marios Kyriakou given that they are easily accessible and mostly have detailed information. This will ensure capturing the rapid evolution of cyber threats within such a period of time and their implications on banks' performance (Jones et al., 2017).

Data collection was a particularly painstaking process. The absence of organized databases and in general the lack of computerization in many services was a decisive factor and affected the healthy realization of this research effort. In order to identify insolvent organizations during the time period defined above, the records were investigated. The absence of an adequate computerization system made the above procedure particularly time-consuming.

The procedure for the final sample was the following: at first, I found in S&P Market Intelligence Platform the financial variables as represented below for the period needed and found 1054 banks with no missing information. Then, from the file that professor in charge of databases of UCY gave me I had 937 banks with cybersecurity data. The number of banks that were found in both files was 303 banks. From those 303 banks needed to find the defuncted banks so I found from reliable sources such us The Federal Deposit Insurance Corporation (FDIC), Bankrate, Forbes only 15 defuncted banks that were in my data so I took another 15 banks from the file to have pairs. Pairs created by matching the total assets of banks 3 years before. For the CAMEL variables I created the relevant ratios to use in the analysis and for the cybersecurity variable I had the excel file that shows if the banks have a policy on cybersecurity in place to protect from cyber-attack, unauthorized access, and data leaks. 7 of the 15 bankrupt banks found to not using cybersecurity policy. 8 of the 15 bankrupt banks found to using cybersecurity policy. On the other hand, 8 of the 15 healthy banks found not using cybersecurity policy and 7 of the 15 healthy banks found to using cybersecurity policy The SIC Codes for the selected banks are 6020, 6021, 6081, 6035.

The econometric variables are the following and represents the CAMEL approach:

i. Total Equity/ Total Assets: The asset/equity ratio indicates the relationship of the total assets of the firm to the part owned by shareholders (owner's equity). This ratio is an indicator of the company's leverage (debt) used to finance the firm.

ii. Non-performing loans (NPLs)/ Assets: non-performing loans reduce the amount of capital that lenders have for subsequent loans. If a bank has 500 loans and 10 of them are non-performing loans —late commercial loans (90 days past due date) or late consumer loans (180 days past due date)—the non-performing loan ratio for this bank would be 1:50, or 2%.

iii. Net Interest Margin: Net interest margin (NIM) is a measure of the net return on the bank's earning assets, which include investment securities, loans, and leases. It is the ratio of interest income minus interest expense divided by earning assets. NIM = Net interest income/Earning assets.

iv. Return on Average Equity (ROAE): extends the ratio of Return on Equity. Instead of the total equity at the end of the period, it takes an average of the opening and the closing balance of equity for some time. It is calculated as Net earnings divided by Average total equity.

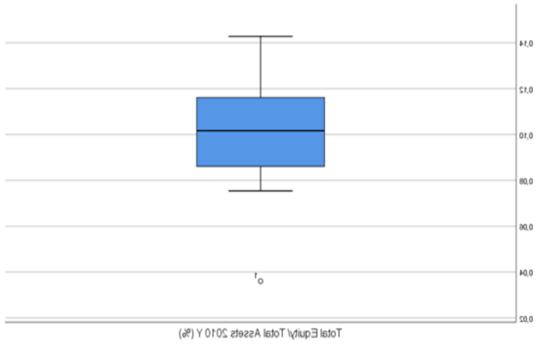
v. Liquid Assets/ Assets: Liquid assets refer to cash on hand, cash on bank deposit, and assets that can be quickly and easily converted to cash. The common liquid assets are stock, bonds, certificates of deposit, or shares.

4.2 Econometric analysis

In this section, testing for the normal distribution of econometric variables has been done. Table 3 (table 3 on appendix) shows that the econometric variables follow the normal distribution since the significance level of the Shapiro – Wilk test is greater than 5%.

Figure 1 shows that there is only one extreme value for the Total Equity/Total Assets variable.

Figure 2 shows that there are four extreme values for the non-performing loans (NPLs)/Assets variable



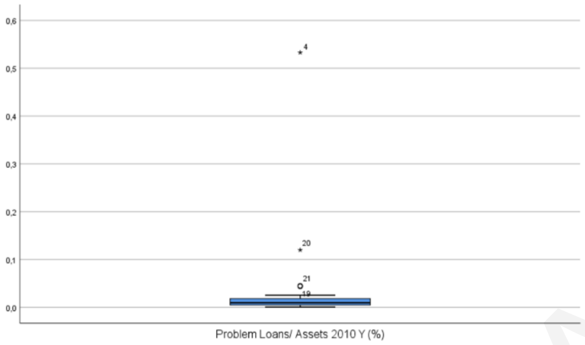
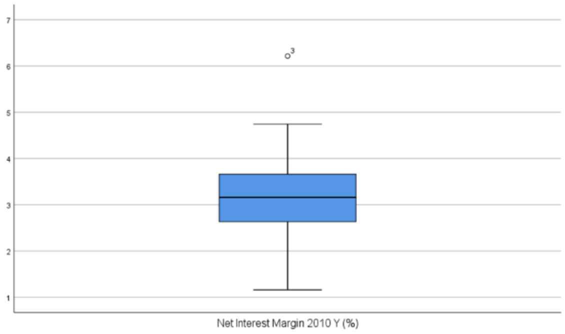


Chart 1: Boxplot for the variable Total Equity/Total Assets

Chart 2: Boxplot for the non-performing loans (NPLs)/ Assets variable

Figure 3 shows that there is an extreme value for the Net Interest Margin variable.

Figure 4 shows that there is no extreme value for the ROAE variable



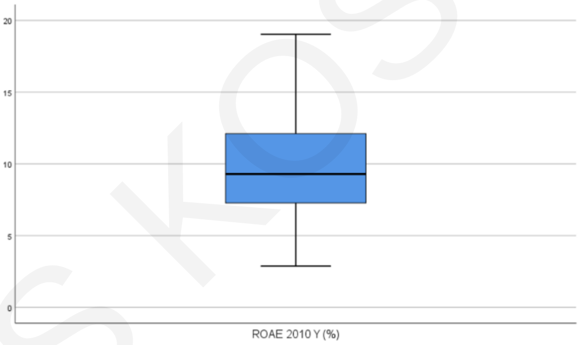


Chart 3: Boxplot for the Net Interest Margin variable

Chart 4: Boxplot for the ROAE variable

Figure 5 shows that there are four extreme values for the Liquid Assets/ Assets variable.

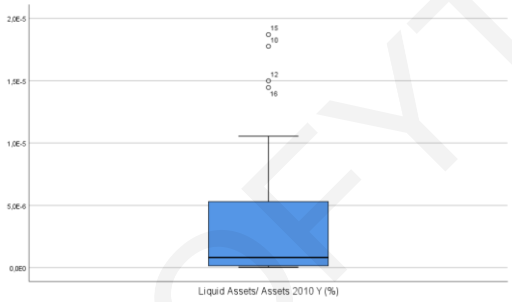
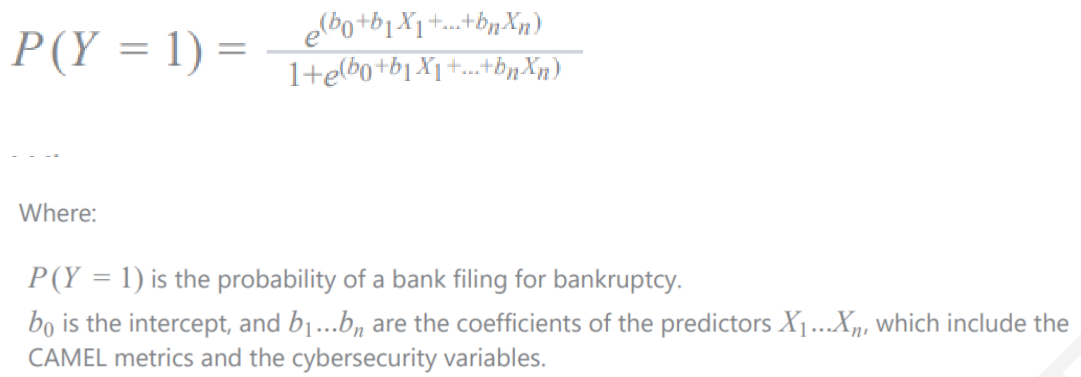


Chart 5: Boxplot for the variable Liquid Assets/ Assets

4.3 Empirical models, measurement of variables and expectations

Relationship existing between the CAMEL metrics, the cybersecurity variables, and bank bankruptcy will be established using a logistic regression model. This is very well supported by the fact that the model under speculation has ample ability to predict dichotomous events such as bankruptcy versus non-bankruptcy (Hosmer, Lemeshow, & Sturdivant, 2013). The form of the equation representing the model will be as follows:



$$P(Y=1)=\frac{e^{(b_0+b_1X_1+...+b_nX_n)}}{1+e^{(b_0+b_1X_1+...+b_nX_n)}}$$

Where:

$P(Y=1)$ is the probability of a bank filing for bankruptcy.
b_0 is the intercept, and $b_1...b_n$ are the coefficients of the predictors $X_1...X_n$, which include the CAMEL metrics and the cybersecurity variables.

Measurement of Variables: For the calculation of each variable, see further explanation in the following table of measurements (table 1 in appendix). For instance, representing "Capital Adequacy" from the CAMEL model is the ratio, Equity Capital to Total Assets. The variables in the field of cybersecurity represented from data collected from the university of Cyprus, stating that a bank has cybersecurity policy or not.

With the increasing exposure to cyber threats, an all-inclusive view of bankruptcy resilience in view banks is called for. By incorporating the classic CAMEL model with the cybersecurity metrics, this paper seeks to hypothetically present a more all-round bank health analysis framework than was possible before especially in the contemporary time.

5. Empirical results

5.1 Descriptive statistics and correlation analysis

Table 4 shows the descriptive statistics of the economic variables of the paired banks. The mean value of Variable Capital Adequacy is 0.1026, indicating that, on average, banks have 10.26% of their assets covered by equity. The standard deviation of 0.0218 suggests relatively low variability in this ratio across the sample. Median is 0.1016, the minimum value of Variable Capital Adequacy is equal to 0.0360 and the maximum value is equal to 0.1428. This ratio is a measure of capital adequacy, which is a crucial component of the CAMEL framework. A higher value typically signifies better financial health and a lower risk of bankruptcy. Relating to Hypothesis 1, a higher Total Equity/Total Assets ratio would correlate with lower bankruptcy risk, aligning with the expectation that effective cybersecurity, alongside strong financial metrics, contributes to reduced bankruptcy risk.

Also, The mean value of non-performing loans/assets is 0.0331, with a relatively high standard deviation of 0.0970, indicating more variability in this ratio across the sample. Median value is 0.0094, the minimum value of non-performing loans/ Assets is equal to 0.0006 and the maximum value is equal to 0.5327. A higher ratio of non-performing loans/assets signifies higher credit risk and potentially indicates financial distress.

This aligns with the hypothesis that deteriorating asset quality, represented by a higher ratio of non-performing loans, increases bankruptcy risk.

Also, The mean NIM is 3.1866, with a standard deviation of 1.0046 and median of 3.1580. NIM measures the profitability of a bank's lending activities and indicates its ability to generate revenue from interest-bearing assets. The minimum value of Net Interest Margin is equal to 1.1581 and the maximum value is equal to 6.2152. A higher NIM suggests better profitability and potentially lower bankruptcy risk, as it reflects a bank's ability to earn income from its core operations.

Additionally, The mean ROAE is 9.5921, with a standard deviation of 3.9704 and median 9.2885. ROAE measures a bank's profitability relative to its equity, indicating its efficiency in generating returns for shareholders. The minimum value of ROAE is equal to 2.8776 and the maximum value is equal to 19.0302. A higher ROAE suggests better performance and potentially lower bankruptcy risk, as it reflects the bank's ability to generate profits from its equity base.

The mean value of liquidity is 27.1882, indicating that on average, 27.19% of the banks' assets are liquid. This suggests a relatively high level of liquidity among the banks. The standard error is 1.934503, reflecting the precision of the mean estimate a smaller value indicates higher precision. The median liquidity value is 25.61556, which is slightly lower than the mean. This suggests that the distribution of liquidity values may be slightly right-skewed, with a few banks having significantly higher liquidity. The standard deviation is 10.59571, showing considerable variability in liquidity levels among the banks. The sample variance, which is the square of the standard deviation, is 112.2691, further emphasizing the diversity in liquidity levels. The range of liquidity values is 54.41925, calculated from a minimum of 4.912957 to a maximum of 59.33221, highlighting the wide disparity between the banks with the lowest and highest liquidity. These statistics collectively indicate that while the average liquidity is relatively high, there is significant variation among banks, with some maintaining very high levels of liquid assets relative to their total assets.

The next tables are the descriptive statistics of healthy and bankrupted banks separately. Healthy banks maintain a higher mean capital adequacy ratio of 0.102445 compared to 0.097849 in bankrupt banks. This indicates that healthy banks have a stronger buffer to absorb potential losses, reflecting better financial stability and lower insolvency risk .In terms of asset quality, healthy banks have a lower mean ratio of non-performing loans to total assets (0.011818) compared to bankrupt banks (0.013504). This suggests that healthy banks are more effective in managing credit risk and maintaining a sound lending portfolio, which contributes significantly to their stability .Management efficiency, measured by the net interest margin, is slightly higher in bankrupt banks (3.245832) compared to healthy banks (3.097518). However, this difference is not substantial enough to be a differentiating factor in bankruptcy risk. Both categories demonstrate the ability to earn a reasonable spread between interest income and expenses, indicating that other factors are more critical in determining financial health. Earnings, represented by the return on average equity (ROAE), are robust in both healthy (10.011557) and bankrupt banks (10.519048). This similarity suggests that while earnings performance is essential, it is not sufficient on its own to prevent bankruptcy if other financial aspects are compromised. Liquidity ratios are comparable between the two groups, with healthy banks at 24.248023 and bankrupt banks at 23.881857. This indicates that maintaining liquidity is necessary for short-term obligations but does not solely determine a bank's risk of bankruptcy.

Table 8 presents the correlation of the paired sample, at a significance level of 5%. Table 8 shows that there is a statistically significant relationship between Total Equity/Total Assets and Net Interest Margin (r = 0.489, p<1%). That is, as the value of Total Equity/Total Assets increases, the value of Net Interest Margin increases. The positive correlation between Total Equity/Total Assets and Net Interest Margin suggests that as the ratio of total equity to total assets increases, the net interest margin also increases. This result aligns with expectations and supports the hypothesis that higher levels of equity relative to assets are associated with improved profitability, as indicated by a higher net interest margin. A higher equity-to-assets ratio signifies better capital adequacy and financial stability, which can enhance a bank's ability to generate profits from its interest-bearing assets. Relating to the hypothesis, this result reinforces the importance of capital adequacy, as captured by the Total Equity/Total Assets ratio, in predicting bank performance and financial health. It suggests that banks with stronger capital positions are better positioned to achieve higher profitability, as reflected by the net interest margin.

Table 8 also shows that there is a statistically significant relationship between ROAE and Net Interest Margin (r = 0.48, p<1%). That is, as the value of ROAE increases, the value of Net Interest Margin increases. Similarly, the positive correlation between ROAE and Net Interest Margin indicates that as the return on average equity increases, the net interest margin also increases. This finding is consistent with expectations and supports the hypothesis that higher returns on equity are associated with improved profitability, reflected in a higher net interest margin. A higher ROAE signifies better performance and efficiency in generating returns for shareholders, which can lead to higher profitability from interest-based activities. Relating to the hypothesis, this result underscores the importance of earnings performance, as captured by ROAE, in predicting bank profitability and financial stability. It suggests that banks with higher returns on equity are more likely to achieve higher net interest margins, contributing to overall financial health.

Next tables show the corelation of healthy and bankrupt banks separately. For healthy banks, the correlation between capital adequacy (C) and other variables shows that there is a moderate positive correlation with management efficiency (M), with a coefficient of 0.440715. This suggests that banks with higher capital adequacy also tend to have better management efficiency, which likely contributes to their stability. The asset quality (A) has a slight positive correlation with capital adequacy (0.13306) and a very weak relationship with management efficiency (0.023103). This indicates that, while asset quality does not strongly correlate with other variables, better capital adequacy and management practices might slightly improve asset quality. Earnings (E) have a weak negative correlation with capital adequacy (-0.092912) and asset quality (-0.08695), but a small positive correlation with management efficiency (0.216043). This implies that higher earnings are not necessarily linked to better capital adequacy or asset quality but are somewhat associated with effective management practices. Liquidity (L) shows a weak negative correlation with capital adequacy (-0.1383) and management efficiency (-0.369784), indicating that higher liquidity is not strongly associated with better capital adequacy or management.

For bankrupt banks, the correlation patterns are somewhat different. The capital adequacy (C) is moderately correlated with management efficiency (0.561329), similar to healthy banks, suggesting that even in distressed situations, better-managed banks maintain higher capital adequacy. Asset quality (A) has a positive correlation with liquidity (0.348833), indicating that banks with poor asset quality might maintain higher liquidity as a precautionary measure. Earnings (E) have a negative correlation with capital adequacy (-0.314311) and asset quality (-0.281359), highlighting that poorer earnings performance is associated with lower capital adequacy and poorer asset quality in bankrupt banks. The positive correlation between earnings and management efficiency (0.214825) again underscores the importance of effective management.

Interestingly, cybersecurity has a positive correlation with capital adequacy (0.13477) and management efficiency (0.168086) in bankrupt banks, but a negative correlation with earnings (-0.26175). This suggests that while cybersecurity measures are present, they are not sufficient to ensure positive earnings outcomes in financially distressed banks. Comparing the two groups, healthy banks generally show weaker correlations between the variables, suggesting a more balanced interplay between them. In contrast, bankrupt banks exhibit stronger correlations, indicating that deficiencies in one area (e.g., capital adequacy or asset quality) are more likely to be associated with deficiencies in other areas, contributing to their financial instability.

Next tables show the test of differences of mean. Capital adequacy, measured by the ratio of Total Equity to Total Assets, shows mean values of 0.102307 for bankrupted banks and 0.102847 for healthy banks. The t-statistic of -0.071589 with a p-value (two-tail) of 0.943942 indicates no statistically significant difference between the two means. This suggests that capital adequacy does not significantly differ between bankrupted and healthy banks, implying that this metric alone may not be a strong indicator of bankruptcy risk. Earnings, represented by the Return on Average Equity (ROAE), have mean values of 8.983404 for bankrupted banks and 10.200706 for healthy banks. The t-statistic of 0.439145 with a p-value of 0.666894 (two-tail) shows no significant difference. This suggests that while healthy banks have a numerically higher ROAE, the difference is not statistically significant. Thus, ROAE might not be a decisive factor in differentiating between bankrupted and healthy banks.

Asset quality, measured by the ratio of non-performing loans (NPLs) to assets, shows mean values of 0.051817912 for bankrupted banks and 0.014462101 for healthy banks. The p-value (two-tail) of 0.295842746 indicates no statistically significant difference, despite the apparent numerical difference. This lack of statistical significance suggests that asset quality, as measured by NPLs, might not strongly differentiate between bankrupted and healthy banks within this sample. Management efficiency, measured by the Net Interest Margin, has mean values of 3.076914 for bankrupted banks and 3.296311 for healthy banks.

The t-statistic of -0.625019 with a p-value of 0.542013 (two-tail) indicates no significant difference. This implies that the ability of management to generate income from interest does not significantly differ between bankrupted and healthy banks.

Liquidity, measured by the ratio of Liquid Assets to Total Assets, shows mean values of 30.43505 for bankrupted banks and 23.94135 for healthy banks. The p-value (two-tail) of 0.1338 indicates no statistically significant difference between the means. This suggests that liquidity levels are similar between bankrupted and healthy banks, implying that liquidity alone may not be a strong indicator of bankruptcy risk. Cybersecurity policy, a binary variable indicating the presence (1) or absence (0) of a policy, shows mean values (proportions) of 0.466667 for bankrupted banks and 0.533333 for healthy banks. The t-statistic of -0.564076 with a p-value of 0.581627 (two-tail) indicates no significant difference. This suggests that having a cybersecurity policy does not significantly correlate with whether a bank is bankrupted or healthy.

The similar capital adequacy ratios between bankrupted and healthy banks suggest that maintaining regulatory equity levels is uniformly critical but not necessarily indicative of a bank’s health status. The similar ROAE values between the two groups indicate that profitability, as measured by ROAE, does not strongly differentiate between bankrupted and healthy banks, highlighting the need for more comprehensive profitability measures. Although there is a numerical difference in NPL ratios, the lack of statistical significance implies that while poor asset quality might be more prevalent in bankrupted banks, it may not be a definitive predictor of bankruptcy risk within this sample. This highlights the importance of considering additional factors alongside NPLs when assessing bank stability. The similar Net Interest Margins suggest that operational efficiency in generating interest income is maintained across both bankrupted and healthy banks, indicating that other management factors might be at play in determining bank health. The similar liquidity ratios indicate that both bankrupted and healthy banks maintain comparable levels of liquid assets, suggesting that liquidity alone is not a significant differentiator. Finally, the lack of significant difference in the presence of cybersecurity policies suggests that while cybersecurity is crucial for risk management, its direct impact on financial health, as measured by these metrics, might not be immediately evident or may require more nuanced measures to capture.

The next table show the test of differences of mean for all the sample (bankrupted and healthy). The mean capital adequacy ratios are 0.097849 for bankrupted banks and 0.102445 for healthy banks. The p-value (two-tail) of 0.022487 indicates a statistically significant difference between the two means. This suggests that capital adequacy, measured by the ratio of Total Equity to Total Assets, is significantly lower in bankrupted banks. Economically, this implies that lower capital adequacy is associated with a higher risk of bankruptcy, highlighting the importance of maintaining sufficient equity levels to absorb potential losses. The mean asset quality ratios (NPLs/Assets) are 0.013504 for bankrupted banks and 0.011818 for healthy banks. The p-value (two-tail) of 0.199323 indicates no statistically significant difference between the two means. Despite the numerical difference, this lack of statistical significance suggests that while poor asset quality might be prevalent in bankrupted banks, it may not be a definitive predictor of bankruptcy risk within this sample. Thus, other factors should also be considered when assessing the risk.

The mean Net Interest Margin for bankrupted banks is 3.245832 and 3.097518 for healthy banks. The p-value (two-tail) of 0.143079 indicates no statistically significant difference between the two means. This implies that the ability to generate income from interest does not significantly differ between bankrupted and healthy banks, indicating that other management factors may influence bank health. The mean ROAE for bankrupted banks is 10.519048, while for healthy banks it is 10.011557. The p-value (two-tail) of 0.209378 indicates no statistically significant difference between the two means. This suggests that profitability, as measured by ROAE, does not significantly differ between bankrupted and healthy banks. Economically, this implies that profitability alone may not be a strong indicator of bankruptcy risk, and other factors must be considered.

The mean liquidity ratios (Liquid Assets/Total Assets) are 23.881857 for bankrupted banks and 24.248023 for healthy banks. The p-value (two-tail) of 0.659909 indicates no statistically significant difference between the two means. This suggests that liquidity levels are similar between bankrupted and healthy banks, implying that liquidity alone may not be a strong indicator of bankruptcy risk. The mean values for cybersecurity policy adoption are 0.866667 for healthy banks and 0.6875 for bankrupted banks. The p-value (two-tail) of 5.06067E-09 indicates a highly significant difference. This suggests that healthy banks are more likely to have robust cybersecurity policies in place compared to bankrupted banks. Economically, this highlights the importance of cybersecurity measures in maintaining the overall health and stability of banks, potentially reducing the risk of cyber-attacks and associated financial losses.

The significant difference in capital adequacy suggests that maintaining higher levels of equity is crucial for mitigating bankruptcy risk. The lack of significant differences in earnings, asset quality, management efficiency, and liquidity implies that these factors alone may not be sufficient indicators of bankruptcy risk, emphasizing the need for a holistic approach. The data suggests that healthy banks are more likely to have strong cybersecurity policies, highlighting the role of cybersecurity in maintaining financial stability.

5.2 Empirical results

In this section, the Logistic Regression test was performed, at a significant level of 5%. In this control the dependent variable is the defunct – healthy and independent variables are the financial variables and cybersecurity variable.

The regression coefficient (B) indicates the direction and magnitude of the relationship between each predictor variable and the dependent variable. A positive B value suggests a positive relationship, whereas a negative B value suggests a negative relationship. The standard error (S.E.) measures the accuracy of the coefficient estimate, with smaller standard errors indicating more precise estimates. The Wald statistic is used to test the null hypothesis that the coefficient is zero, larger values suggest that the coefficient is significantly different from zero. The significance level (Sig.), or p-value, tests the null hypothesis that the coefficient equals zero, with a p-value less than 0.05 typically indicating a significant association between the predictor and the dependent variable. The odds ratio (Exp(B)) represents the change in odds resulting from a one-unit change in the predictor variable, where an odds ratio greater than 1 indicates increased odds and an odds ratio less than 1 indicates decreased odds. The 95% confidence interval for Exp(B) provides a range within which the true odds ratio is expected to fall 95% of the time. If this interval includes 1, the predictor may not be significantly associated with the outcome.

Table 24 shows that the model of the paired sample is not well fitted, since the coefficient of determination of the model is equal to 0.159. The low coefficient of Cox & Snell R Square (0.159) in Table 24 indicates that the model is not well-fitted, suggesting that the predictors included in the model may not adequately explain the variation in the dependent variable. The low Cox & Snell R Square suggests that the predictors included in the model have limited explanatory power in predicting the outcome variable. A poor model fit can undermine the reliability and validity of the predictive model, limiting its utility in accurately assessing the risk of bankruptcy. Relating to the hypothesis, the poor model fit suggests that the selected predictors may not capture the full spectrum of factors influencing bankruptcy risk. This outcome may indicate a need to reassess the choice of predictors and potentially incorporate additional variables or refine the model's specifications to improve predictive accuracy.

Previous studies in bankruptcy prediction have demonstrated the importance of selecting relevant predictors and model specifications to achieve accurate predictions. For example, research by Charitou (2015) and Jordan et al. (2010) highlights the significance of financial indicators in predicting bank failures, emphasizing the need for comprehensive models that consider multiple factors. The poor model fit observed in Table 24 underscores the challenges inherent in developing effective bankruptcy prediction models and the importance of continued research efforts to improve model performance.

Table 24 shows that none of the financial indicators or cybersecurity variable has an effect on the defunct – healthy variable, since the significance level is greater than 5%. The absence of significant effects suggests that the financial indicators and the cybersecurity variable included in the analysis do not significantly influence the bankruptcy variable. This outcome may indicate that the chosen predictors are not strong determinants of bankruptcy risk in the context of the model. It's essential to consider potential reasons for this lack of significance, such as the choice of predictors, sample size, model specification, or the presence of confounding variables.

Relating to hypothesis, if the hypothesis posited that financial indicators and cybersecurity metrics would have a significant effect on bankruptcy risk, the lack of significance suggests that this hypothesis are not supported by the data. This outcome might prompt a reassessment of the conceptual framework underlying the hypothesis or a reconsideration of the variables included in the analysis. Table 24 shows that none of the financial indicators or the cybersecurity variable have a significant effect on the dependent variable, implying that the presence of a cybersecurity policy does not significantly influence bankruptcy risk. This result is inconsistent with the expectation outlined in the hypothesis.

The unexpected result challenges the assumption that effective cybersecurity measures directly mitigate bankruptcy risk. It suggests that while cybersecurity is crucial for protecting against cyber threats, its impact on overall financial stability and bankruptcy risk may be more nuanced than previously assumed. Possible explanations for this discrepancy could include the effectiveness of the cybersecurity measures implemented, the complexity of the relationship between cybersecurity and financial risk, or the presence of unaccounted confounding variables.

Previous research in bankruptcy prediction has highlighted the importance of selecting relevant predictors and employing robust modeling techniques to achieve accurate predictions. Studies such as those by Charitou (2015) and Jordan et al. (2010) have demonstrated the significance of financial indicators in predicting bank failures. The lack of significant effects observed in Table 24 underscores the challenges inherent in developing effective bankruptcy prediction models and the need for continued research to refine model specifications and improve predictive accuracy.

Based on the results presented, Hypothesis 1, which posits that the policy on cybersecurity negatively affects bankruptcy risk among banks, is not supported. The analysis indicates that none of the financial indicators or the cybersecurity variable included in the model have a significant effect on the defunct – healthy variable, with significance levels greater than 5%.

Furthermore, the lack of significant effects suggests that the chosen predictors, including cybersecurity measures, do not significantly influence bankruptcy risk within the context of the model. This implies that the data did not provide evidence to support the hypothesis that forward investment in cybersecurity correlates negatively with bankruptcy risk among banks.

The analysis suggests potential reasons for the lack of significance, such as the choice of predictors, sample size, model specification, or the presence of confounding variables. It's essential to reflect on these factors and consider potential limitations or biases in the analysis. Therefore, based on the results presented, Hypothesis 1 is not supported by the data.

According to empirical findings from logistic regression analysis, however, the outcome does not support any statistically significant relationship at all that exists with classic financial indicators inclusive of cybersecurity metrics against the current bankrupt status for organisations. This absence of a significant correlation threatens the initial postulation that direct investment in cybersecurity would transpire as an observable reduction in risk of bankruptcy. This suggests that while investment in cybersecurity may be important, the direct relationship it shares with leading to bankruptcy is perhaps not so linear or may be moderated by some other factors which are not applied herein.

According to the study, the ratio of Total Equity to Total Assets was higher in organizations that had a cybersecurity policy as opposed to those without having such a policy. While this does not directly validate the hypothesis, it implies an indirect relationship in a way that cybersecurity readiness could influence the opinions of the investors and stakeholders towards the financial well-being of an organization. While it does not directly pin down a causal relationship between higher cybersecurity scores and overall financial health, it implies that the observed correlation for higher cybersecurity precautions may be reflecting an indirect effect on financial stability.

This finding contributes to existing literature by highlighting the need for a more comprehensive understanding of the relationship between cybersecurity measures and bankruptcy risk in the banking sector. It underscores the importance of considering multiple factors beyond cybersecurity alone when assessing financial stability and bankruptcy risk. Future research could delve deeper into the mechanisms underlying this relationship and explore potential moderating or mediating variables to provide a more nuanced understanding of the interplay between cybersecurity and financial risk.

In conclusion, the details of the study provide valuable insights on the interplay of cybersecurity with financial health, but the results do not affirm conclusively nor deny the proposed hypothesis. The results point towards a more complex relationship between cyber risk protective measures and financial stability than has been expected before, highlighting the need for conducting further studies to explore these complexities, and to develop more forward-looking models for the today financial risk assessment.

On the other hand, logistic regression was performed with all the sample data, containing all the healthy banks. The logistic regression model examining the probability of bank default reveals that cybersecurity is a critical factor, with the binary variable for cybersecurity policies showing a highly significant positive relationship with default probability. The model's -2 Log Likelihood value is 1159.761, and it achieves Cox & Snell R Square and Nagelkerke R Square values of 0.011 and 0.035, respectively, indicating that the model explains a modest portion of the variance in default probability. Specifically, the presence of cybersecurity policies significantly reduces the likelihood of default, with an odds ratio of 2.824, suggesting that banks without such policies are about 2.8 times more likely to default. This underscores the importance of robust cybersecurity measures for banks, highlighting their role in risk management, regulatory compliance, and financial stability. Regulators and policymakers should enforce stringent cybersecurity standards to mitigate default risks, while banks should integrate comprehensive cybersecurity strategies into their risk management frameworks to ensure long-term resilience and maintain investor confidence.

Variable Capital Adequacy in the logistic regression model has a regression coefficient (B) of -10.467 with a standard error of 3.945. The Wald statistic for Variable Capital Adequacy is 7.040, and the p-value is 0.008, indicating that it is significantly associated with the probability of default at the 1% level. The odds ratio (Exp(B)) for Variable Capital Adequacy is 0.000. This suggests that Variable Capital Adequacy has a significant negative relationship with the probability of default, where an increase in Variable Capital Adequacy drastically decreases the odds of the bank defaulting.

In contrast, Variable Asset quality has a regression coefficient (B) of 1.564 and a standard error of 1.877. The Wald statistic is 0.695, with a p-value of 0.405, indicating that Variable Asset quality is not significantly associated with the probability of default. The odds ratio (Exp(B)) is 4.779. This implies that while Variable Asset quality shows a positive relationship with the probability of default, the association is not statistically significant.

Variable Management shows a regression coefficient (B) of 0.182 and a standard error of 0.093, with a Wald statistic of 3.835 and a p-value of 0.050, making it marginally significant. The odds ratio (Exp(B)) for Variable Management is 1.199. This suggests that a one-unit increase in Variable Management slightly increases the odds of default, but the relationship is only marginally significant. Variable Earnings, with a regression coefficient (B) of 0.001 and a standard error of 0.017, has a Wald statistic of 0.002 and a p-value of 0.956, indicating no significant association with the probability of default. The odds ratio (Exp(B)) for Variable Earnings is 1.001, suggesting no substantial effect on the odds of default.

The economic and financial implications of these findings are significant. Variables that are statistically significant in the logistic regression model, such as Variable C, indicate factors that likely influence the probability of default. Understanding these relationships helps in making informed decisions, such as focusing on reducing Variable C to decrease the likelihood of default. Policymakers can use these insights to implement strategies targeting significant variables to reduce the risk of default among banks. Furthermore, identifying variables that negatively impact the probability of default aids in better risk management and mitigation strategies. This detailed analysis provides a comprehensive understanding of the predictors' influence on the probability of default, essential for strategic planning and decision-making in the financial sector.

Variable Liquidity has a regression coefficient (B) of -0.003, indicating a very slight negative relationship with the probability of default. The standard error (S.E.) of 0.008 suggests that this estimate has a reasonable level of precision. The Wald statistic of 0.123, coupled with a significance level (Sig.) of 0.726, indicates that Variable Liquidity is not statistically significant in predicting the probability of default. The p-value is well above the common threshold of 0.05, meaning that we cannot reject the null hypothesis that the coefficient for Variable Liquidity is zero. The odds ratio (Exp(B)) for Variable "L" is 0.981, which is very close to 1. This suggests that a one-unit change in Variable Liquidity has a negligible effect on the odds of default. Essentially, Variable Liquidity does not appear to have a meaningful impact on the probability of a bank defaulting based on this model.

The logistic regression model examining the probability of bank default includes a significant binary variable related to cybersecurity. This cybersecurity variable takes the value of 1 if the bank has a policy in place to protect from cyber-attacks, unauthorized access, and data leaks, and 0 if the bank does not have such a policy.

The regression coefficient (B) for the cybersecurity variable is 1.038, indicating a positive relationship with the probability of bank default. This means that banks without a cybersecurity policy in place (value of 0) are more likely to default compared to banks with a cybersecurity policy (value of 1). The standard error (S.E.) is 0.246, suggesting that this estimate is reasonably precise. The Wald statistic of 17.881, coupled with a significance level (Sig.) of less than 0.001, indicates that the cybersecurity variable is highly statistically significant in predicting the probability of default. The very low p-value allows us to confidently reject the null hypothesis that the coefficient for the cybersecurity variable is zero.

The odds ratio (Exp(B)) for the cybersecurity variable is 2.824. This implies that the odds of a bank defaulting are approximately 2.8 times higher for banks without a cybersecurity policy compared to those with one. The significant positive coefficient for the cybersecurity variable underscores its critical role in influencing the probability of bank default. This finding has profound economic and financial implications. Firstly, it highlights the importance of robust cybersecurity measures within the banking sector for effective risk management and mitigation. Banks without cybersecurity policies are significantly more likely to default, stressing the need for banks to invest in developing and implementing comprehensive cybersecurity policies and infrastructure. Effective cybersecurity can prevent financial losses, protect customer data, and maintain operational integrity, thereby reducing the likelihood of default.

Secondly, these findings have important policy implications. Regulators and policymakers need to enforce stringent cybersecurity standards and compliance measures across the banking sector. By doing so, they can help ensure that all banks adhere to best practices in cybersecurity, thus safeguarding the financial system against potential disruptions caused by cyber threats. Furthermore, a bank's cybersecurity stance can significantly influence investor confidence. Banks with strong cybersecurity policies are likely to be viewed as lower risk, attracting more investment. Conversely, banks without adequate cybersecurity measures might face higher borrowing costs and reduced investor interest due to the perceived higher risk of default.

For bank management, these findings highlight the importance of incorporating cybersecurity into strategic planning and risk management frameworks. Regular assessments of cybersecurity measures, investment in advanced cybersecurity technologies, and continuous monitoring of cyber threats are essential strategies to enhance bank stability and reduce the probability of default. At a macro level, the overall stability of the financial system is closely tied to the cybersecurity health of individual banks. A systemic approach to strengthening cybersecurity across all financial institutions can contribute to the resilience of the financial system, protecting against widespread disruptions that could arise from cyberattacks.

Overall, the empirical results support the theoretical frameworks underpinning the study. Modern Portfolio Theory (MPT) and the Efficient Market Hypothesis (EMH) suggest that incorporating cybersecurity information can affect market valuations and financial stability. The positive correlation between cybersecurity policy and the Total Equity/Total Assets ratio aligns with the principle that diversification, including investment in cybersecurity, mitigates risks. This result supports the hypothesis that effective cybersecurity enhances a bank's financial health and stability. Information asymmetry, as highlighted in Akerlof’s "Market for Lemons," is evident in the lack of significant differences in some financial indicators between healthy and bankrupt banks. This underscores the need for transparency in cybersecurity measures to reduce information asymmetry and inform stakeholders more accurately. The findings suggest that while traditional financial metrics alone may not fully capture a bank’s risk profile, integrating cybersecurity measures provides a more comprehensive assessment.

The Gordon-Loeb Model advocates for appropriate investment in cybersecurity, and the empirical results showing higher Total Equity/Total Assets ratios in organizations with cybersecurity policies align with this model. This indicates that strategic investment in cybersecurity contributes to financial resilience, supporting the integration of cybersecurity metrics into traditional financial models. Considering systemic risk factors, as discussed by De Bandt and Hartmann, the significant impact of cybersecurity policies on reducing default risk underscores the importance of cybersecurity in mitigating systemic risk within the banking sector. This reinforces the need for comprehensive risk management strategies that include cybersecurity measures to ensure financial stability.

The importance of capital adequacy and its significant negative relationship with default risk align with the Basel Committee on Banking Supervision's (BCBS) guidelines, which emphasize stability in funding and liquidity, including considerations of cyber risks. This supports the argument that robust cybersecurity measures are integral to maintaining regulatory compliance and financial stability. The empirical results also reflect the significance of adhering to international standards such as the General Data Protection Regulation (GDPR) and the Federal Financial Institutions Examination Council (FFIEC) guidelines, which emphasize the importance of cybersecurity in managing financial risks. The finding that banks with cybersecurity policies have higher Total Equity/Total Assets ratios supports the notion that compliance with stringent cybersecurity standards enhances financial stability.

The study by Charitou (2015) on the importance of new performance measures for predicting bank default is complemented by the current findings. The inclusion of cybersecurity metrics in the bankruptcy prediction model enhances the model's ability to anticipate risks, aligning with the evolving landscape of cybersecurity threats in the banking sector. Jordan et al. (2010) found that specific variables can predict bank failure, and incorporating cybersecurity as an additional variable could further enhance the model’s accuracy. The current study’s findings that organizations with cybersecurity policies have better financial health support this integration, suggesting that cybersecurity measures are crucial in predicting and preventing bank failures.

The descriptive statistics show that organizations with a cybersecurity policy have a higher Total Equity/Total Assets ratio. This suggests that banks with robust cybersecurity policies tend to have better capital adequacy, which is critical for financial stability. The positive correlation between Total Equity/Total Assets and the presence of a cybersecurity policy supports the hypothesis that effective cybersecurity measures contribute to a bank's financial health and reduce bankruptcy risk. The t-test results show a statistically significant relationship between the Total Equity/Total Assets ratio and the presence of a cybersecurity policy. This indicates that banks with cybersecurity policies have stronger capital positions, aligning with the hypothesis that cybersecurity investment enhances financial stability and reduces bankruptcy risk.

The logistic regression analysis shows that the presence of a cybersecurity policy significantly reduces the likelihood of bank default, with an odds ratio indicating that banks without cybersecurity policies are about 2.8 times more likely to default. This highly significant positive relationship between cybersecurity policies and reduced default probability strongly supports the hypothesis that cybersecurity measures mitigate bankruptcy risk. Despite the significant relationship between cybersecurity policies and reduced default probability, the overall model fit (Cox & Snell R Square and Nagelkerke R Square) is modest, indicating that while cybersecurity is a critical factor, other variables also play important roles in predicting bank bankruptcy. This suggests that while the hypothesis is supported, the model could be improved by incorporating additional relevant factors.

6. Conclusions, Limitations, and Future Research

6.1 Conclusions

The present study embarked an exploratory journey with an objective to integrate the classic financial indicators with the emerging cybersecurity metrics for foretelling bankruptcy in the banking sector. The major findings point out the complexity and ever-changing kind as far as financial risk is concerned in the digital age.

First, the research has shown that there is no statistically significant relationship between the analyzed financial indicators (Total Equity / Total Assets, non-performing loans/ Assets, Net Interest Margin, Return on Average Equity, Liquid Assets / Assets) or the cybersecurity variable and the bankruptcy status of organizations. After testing all the available sample found that the presence of cybersecurity policies significantly reduces the likelihood of bank default, with banks lacking such policies being approximately 2.8 times more likely to default. This underscores the crucial role of robust cybersecurity measures in mitigating default risk, suggesting that banks should prioritize developing and implementing comprehensive cybersecurity strategies. The highly significant positive relationship between cybersecurity and default probability emphasizes the need for stringent regulatory standards to ensure banks' cybersecurity readiness.

The analysis reveals that capital adequacy has a significant negative relationship with default probability, indicating that higher capital adequacy drastically lowers the odds of default. This finding supports the importance of maintaining strong capital reserves as a buffer against financial instability. In contrast, variables such as asset quality, management, earnings, and liquidity were not found to have significant impacts on default probability. Interestingly, organizations that adopted cybersecurity policies had higher Total Equity/Total Assets ratios compared to those without such policies. This outcome emphasizes the increasing importance of cybersecurity to the financial health of firms and strengthens the findings by Romanosky

(2016) regarding the financial loss related to cyber incidents. It implies that investors and stakeholders may view cybersecurity as a symbol of resilience and stability, providing valuable insights for policymakers and bank managers on the importance of integrating cybersecurity and capital adequacy to maintain financial stability and reduce default risk. Moreover, this study has found that the Total Equity/Total Assets and Return on Average Equity reveal a positive relationship with Net Interest Margin meaning the intertwined connections for analyzing the financial health indicators considered in the paper.

However, despite these insights, the study faces limitations primarily on its inability to establish a direct casual link between cybersecurity metrics and bankruptcy risk due to data constraints as well as stepping stones of operationalizing cybersecurity investments. This limitation points out how intricate the nature of cyber risk is as a factor towards financial stability as discussed by Gordon and Loeb (2002).

6.2 Limitations

The present research, even though it has offered insightful aspects on the inclusion of cybersecurity metrics along with conventional financial indicators for forecasting the likelihood of bankruptcy, has certain limitations to be delineated.

Primarily, the major limitation can be termed as being the data choice. Relying only on publicly available financial data, and cyber security metrics may fail to portray the entire complex dimension of firm's cyber posture. Indeed, cybersecurity investments are rarely ever fully disclosed in public records and metrics like 'Cybersecurity Expenditure' or 'Cybersecurity Risk Assessment Score' widely differ on how they are reported and interpreted across the length and breadth of organizations. This variation may give inconsistencies in the data as identified by Romanosky (2016) from his cost flow analysis from cyber incidents. Besides, these are standardized financial indicators, but may not be wholly indicative of the fast changes taking place out in the financial environment particularly with the onset of digital transformation as opined by Beaver (1966).

Further, the majorly quantitative methodological approach might neglect the quality aspect of cybersecurity including policy effectiveness, employee awareness, and quality of risk management practices of cyber management. McAfee and Brynjolfsson (2017) argue that the fact that qualitative aspects of digital transformation including cybersecurity can be as important as its quantitative around.

Moreover, the time scale the study examines between ten years is extensive but may be inadequate to be able to reflect full implications regarding long-lasting effects cybersecurity issues have on financial health. Cybersecurity threats and technologies evolve rapidly while implication of such changes upon the financial stability may manifest over a more extended period as analysed cyber risks in insurance business by Eling and Schnell (2016).

In conclusion, although this study advanced understanding in the field of financial risk management through incorporating cybersecurity metrics, its limitations point to the need for more nuanced research methodologies and broader data sets as well as longitudinal studies to provide for deeper and more comprehensive understandings of how cybersecurity impacts financial stability.

6.3 Proposed Areas for Future Research

The results have identified the limitations of this study, and hence several areas that could be pursued in future research represent crucial aspects of further research to facilitate a more holistic view of the cross-effects between cybersecurity and financial health.

i. Expansion of the Datasets and Sector Coverage: Future research is advisable to use a larger, diversified dataset of banks from a range of geographical regions or potentially other financial institutions or sectors that are vulnerable to cyber violations. As cyber risks and the regulatory environments among different countries differ, a wider database would yield more generalizable insights adhering to remarks made by Romanosky (2016). Longitudinal studies that is covering even longer time spans would equally be beneficial to track the dynamism of cybersecurity themes in the face of rapidly growing changes and challenges because of cyber threats as postulated by Eling and Schnell (2016).

ii. Analysis, Based on Qualitative Methods: Introduction of the qualitative research methods that include interviews and case studies with representatives of banks and experts in the cybersecurity field would allow receiving more intricate ideas what follows the implementation of cybersecurity policies in an organization as well as how organizational members perceive its practice within the agency. On the other hand, McAfee and Brynjolfsson (2017) underline that more qualitative insights, which are susceptible to the analysis of consequences flowing from digital transformations, may be not very useful in terms of efficiency estimation of cybersecurity precautions in this way.

iii. Cybersecurity Investment and Policy Effectiveness: The research will need to be able to display to just what extent the flow of investment in cybersecurity can create a reduction in financial risks. This could be researched into the optimal level of spending on cybersecurity for banks as proposed to study how different level of spending and also the strategy or policy will influence financial stability by Gordon and Loeb (2002).

iv. Development of Sophisticated Predictive Models: It is pertinent that development of sophisticated predictive models be developed incorporating an extensive range of cybersecurity metrics with financial indicators. Complex datasets can be analysed, providing more nuanced predictions of risk of bankruptcy, using machine learning/artificial intelligence techniques. This approach aligns with the evolution in FinTech and advanced analytics across the financial services, as positioned by Arner, Barberis and Buckley (2016).

v. Regulatory Impact Analysis: Such analyses on impacts of regulations upon future evolution of financial health of banks, emerging from evolving cybersecurity regulations, should be performed as well. For example, this can be done by evaluating the effectiveness of regulation mechanisms such as the ones in the GDPR and their counterparts issued by Basel Committee in the enhancement of cyber-security practices geared to the reduction of financial risks as noted by Voigt and Von dem Bussche (2017).

vi. Market Perception and Cyber Risk Disclosure: An inquiry in which the key aim would be to attempt to demonstrate how market perception and investor behavior with regard to banks may be useful informing about cyber risk disclosure and practices surrounding the same cyber risks. This research shall seek to establish whether open reporting of cybersecurity mechanisms and measures impact investor confidence and market valuation as posit by Beaver (1966) in his study on financial indicators and investor behavior.

Finally, the research in this field in the future should be conducted on this basis and performed by both quantitative and qualitative methods with the use of new analysis techniques in order to reach the holistic view of the role of cybersecurity in financial stability.

References

Akerlof, G. A. (1970). The Market for "Lemons": Quality Uncertainty and the Market Mechanism. *The Quarterly Journal of Economics*, *84*(3), 488–500.

Arner, D. W., Barberis, J., & Buckley, R. P. (2016). The Evolution of FinTech: A New Post-Crisis Paradigm? *Georgetown Journal of International Law*, 47(4), 1271-1319.

Basel Committee on Banking Supervision. (2010). *Basel III: The Net Stable Funding Ratio*. Bank for International Settlements.

Basel Committee on Banking Supervision. (2018). *Cyber-resilience: Range of practices*. Bank for International Settlements.

Beaver, W. H. (1966). Financial Ratios As Predictors of Failure. *Journal of Accounting Research*, *4*, 71–111.

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of Cyber Risk: An Empirical Analysis. *The Geneva Papers on Risk and Insurance - Issues and Practice*, 40(1), 131-158.

Böhme, R., & Kataria, G. (2006). *Models and Measures for Correlation in Cyber-Insurance*. Workshop on the Economics of Information Security.

Calder, A., & Watkins, S. (2012). *IT Governance: An International Guide to Data Security and ISO27001/ISO27002*. Kogan Page Publishers.

Charitou, S., (2015). Factors Affecting the Probability of Default of US Banks: An Empirical Analysis. *London School of Economics.*

Darrat, A. F., Gray, S., Park, J. C., & Wu, Y. (2016). Corporate Governance and Bankruptcy Risk. *Journal of Accounting, Auditing & Finance,* 31(2), 163-202.

De Bandt, O., & Hartmann, P. (2000). Systemic risk: A survey. European Central Bank *Working Paper, No. 35.*

Demirgüç-Kunt, A., Detragiache, E., & Merrouche, O. (2013). Bank Capital: Lessons from the Financial Crisis. *Journal of Money, Credit and Banking*, 45(6), 1147-1164.

Eling, M., & Schnell, W. (2016). What Do We Know About Cyber Risk and Cyber Risk Insurance? *The Journal of Risk Finance*, 17(5), 474-491.

European Central Bank. (2019). *Cyber resilience oversight expectations for financial market infrastructures.*

Fama, E. F. (1970). Efficient Capital Markets: A Review of Theory and Empirical Work. *The Journal of Finance*, 25(2), 383-417.

Federal Financial Institutions Examination Council (FFIEC). (2017). *Cybersecurity Assessment Tool.* FFIEC IT Examination Handbook.

Gatzlaff, K. M., & McCullough, K. A. (2010). The Effect of Data Breaches on Shareholder Wealth. *Risk Management and Insurance Review*, 13(1), 61-83.

Gerlach, J. (2019). Germany’s Federal Office for Information Security (BSI): Roles and Responsibilities. *Cybersecurity in Germany*.

Gordon, L. A., & Loeb, M. P. (2002). The Economics of Information Security Investment. *ACM Transactions on Information and System Security*, 5(4), 438-457.

Hosmer, D. W., Lemeshow, S., & Sturdivant, R. X. (2013). *Applied Logistic Regression* (3rd ed.). John Wiley & Sons.

Jones, S., Johnstone, D., & Wilson, R. (2017). Predicting Corporate Bankruptcy: An Evaluation of Alternative Statistical Frameworks. *Journal of Business Finance & Accounting*, 44(1-2), 3-34.

Jordan, D. J., Rice, D., Sanchez, J., Walker, C., & Wort, D. H. (2010). Predicting bank failures: Evidence from 2007 to 2010. *Available at SSRN 1652924*.

Markowitz, H. (1952). Portfolio Selection. *The Journal of Finance*, 7(1), 77-91.

McAfee, A., & Brynjolfsson, E. (2017). *Machine, Platform, Crowd: Harnessing Our Digital Future*. W.W. Norton & Company.

Ohlson, J. A. (1980). Financial Ratios and the Probabilistic Prediction of Bankruptcy. *Journal of Accounting Research*, 18(1), 109-131.

Romanosky, S. (2016). Examining the Costs and Causes of Cyber Incidents. *Journal of Cybersecurity*, 2(2), 121-135.

Schinasi, G. J., & Teixeira, P. G. (2006). The Lender of Last Resort in the European Single Financial Market. *International Monetary Fund Working Paper.*

Shapiro, S. S., & Wilk, M. B. (1965). An analysis of variance test for normality (complete samples). *Biometrika*, 52(3/4), 591-611.

Shumway, T. (2001). Forecasting Bankruptcy More Accurately: A Simple Hazard Model. *The Journal of Business*, 74(1), 101-124.

S&P Global Market Intelligence. (2021).

Voigt, P., & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR*). Springer.

Wharton Research Data Services (WRDS). (2021).

Wooldridge, J. M. (2015). *Introductory Econometrics: A Modern Approach (6th ed.).* Cengage Learning.

Appendix

Table 1: Variable definition

List of all variables with their definitions and sources of data

Variable	description and sources of data
Dependent variable	Is binary and has the value of 1 if the bank is defuncted (defaulted) and the value of 0 if the bank is still operating (healthy). [Source: S&P Market Intelligence Platform, The Federal Deposit Insurance Corporation (FDIC), Bankrate, Forbes]
Capital adequacy	**Total Equity / Total Assets** This ratio evaluates the bank's capital relative to its risk-weighted assets. It assesses whether the bank has enough capital to absorb potential losses and maintain solvency. [Source: S&P Market Intelligence Platform - Total Equity code 329641 and Total Assets code 329639]
Asset quality	**Non-performing loans (NPLs)/ Assets** This ratio examines the quality of the bank's assets, including the level of non-performing loans, loan loss reserves, and other indicators of credit risk. [Source: S&P Market Intelligence Platform - Non-performing loans code 299985 and Total Assets code 329639]
Management	**Net Interest Margin** This aspect assesses the competence and effectiveness of the bank's management team in overseeing operations, implementing risk management practices, and making strategic decisions. [Source: S&P Market Intelligence Platform – NIM code 273784]
Earnings	**ROAE (Return on Average Equity)** **(**ROAE=Net Income / Average Shareholders′ Equity × 100) This ratio evaluates the bank's profitability, including its ability to generate income relative to its expenses, as well as the sustainability of its earnings over time. [Source: S&P Market Intelligence Platform – ROAE code 329655]
Liquidity	**Liquid Assets / Assets** This ratio measures the bank's ability to meet its short-term obligations without incurring excessive costs or relying on external sources of funding. It assesses the availability of liquid assets to cover liabilities. [Source: S&P Market Intelligence Platform – Liquid Assets code 274102 and Total Assets code 329639]
Cybersecurity policy	Is binary and has the value of 1 if the bank is using policy on cybersecurity in place to protect from cyber-attack, unauthorized access, and data leaks and the value of 0 if the bank is not using cybersecurity policy. [Source: UCY databases after communication with the relevant department and the professor in charge Mr. Marios Kyriakou]

Table 2: Sample Construction

Banks with CAMEL data from S&P Market Intelligence Platform and for the variable cybersecurity collected from the UCY databases after communication with the relevant department and the professor in charge Mr. Marios Kyriakou. The SIC Codes for the selected banks are 6020, 6021, 6081, 6035. At first, I found in S&P Market Intelligence Platform the CAMEL variables for the period needed and found 1054 banks with no missing information. Then, from the file that professor in charge of databases of UCY gave me I had 937 banks with cybersecurity data. The number of banks that were found in both files was 303 banks. From those 303 banks needed to find the defuncted banks so I found from reliable sources such us The Federal Deposit Insurance Corporation (FDIC), Bankrate, Forbes only 15 defunct banks that were in my data, so I took another 15 banks from the file to have pairs. Pairs created by matching the total assets of operating/defuncted banks 3 years before the bankruptcy of the defuncted bank. For the CAMEL variables I created the relevant ratios to use in the analysis and for the cybersecurity variable I had the excel file that shows if the banks have a policy on cybersecurity in place to protect from cyber-attack, unauthorized access, and data leaks.

	Sample Selection Procedure (Period:2013-2022)	Banks
1	Data for banks from S&P Market Intelligence Platform with not missing information	1054
2	Data for Cybersecurity policy from UCY database file	937
3	Banks that found in both files to have full information	303
4	Bankrupt banks that are in both files	15
5	Operating banks that selected to have pairs	15
	Final Sample	30

SIC CODES	Number of Banks
6020	25
6021	2
6035	2
6081	1

	Number of Banks
Bankrupt with Cybersecurity	8
Bankrupt without Cybersecurity	7
Healthy with Cybersecurity	7
Healthy without Cybersecurity	8

Table 3: Testing for normal distribution

This table shows the results of the test for normal distribution among the variables of all the factors of the CAMEL Model. C is the variable of Capital adequacy and is the Total Equity / Total Assets, A is the Asset quality and is the non-performing loans (NPLs)/ Assets, M is the Management and is the Net Interest Margin, E is the Earnings and is the ROAE, L is the Liquidity and is the Liquid Assets / Assets.

**this is a lower bound of the true significance.*

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	statistic	Df	Sig.	Statistic	df	Sig.
C	,104	30	,200*	,953	30	,204
A	,398	30	<.001	,312	30	<.001
M	,088	30	,200*	,963	30	,379
E	,090	30	,200*	,975	30	,690
L	,287	30	<.001	,693	30	<.001

Table 4: Descriptive statistics of pairs (15 bankrupt and 15 healthy banks)

This table shows the descriptive statistics of all the factors of the CAMEL Model and cybersecurity variable of the paired sample which includes 15 bankrupted banks and 15 healthy.. C is the variable of Capital adequacy and is the Total Equity / Total Assets, A is the Asset quality and is the non-performing loans (NPLs)/ Assets, M is the Management and is the Net Interest Margin, E is the Earnings and is the ROAE, L is the Liquidity and is the Liquid Assets / Assets. Cybersecurity is binary and has the value of 1 if the bank is using policy on cybersecurity in place to protect from cyber-attack, unauthorized access, and data leaks and the value of 0 if the bank is not using cybersecurity policy.

	C	*A*	*M*	*E*	*L*	*CYBERSECURITY*
Mean	0.102577	0.03314	3.186613	9.592055	27.1882	0.5
Standard Error	0.003976	0.017708	0.183415	0.724892	1.934503	0.092848
Median	0.10164	0.009388	3.15804	9.288493	25.61556	0.5
Standard Deviation	0.02178	0.096988	1.004605	3.970397	10.59571	0.508548
Sample Variance	0.000474	0.009407	1.009231	15.76405	112.2691	0.258621
Range	0.106801	0.532132	5.057054	16.15256	54.41925	1
Minimum	0.035958	0.000567	1.158141	2.877627	4.912957	0
Maximum	0.142759	0.532699	6.215195	19.03019	59.33221	1

Table 5: Descriptive statistics of all healthy banks found in both files.

This table shows the descriptive statistics of all the factors of the CAMEL Model and cybersecurity variable of all the available healthy banks found in both files. C is the variable of Capital adequacy and is the Total Equity / Total Assets, A is the Asset quality and is the non-performing loans (NPLs)/ Assets, M is the Management and is the Net Interest Margin, E is the Earnings and is the ROAE, L is the Liquidity and is the Liquid Assets / Assets. Cybersecurity is binary and has the value of 1 if the bank is using policy on cybersecurity in place to protect from cyber-attack, unauthorized access, and data leaks and the value of 0 if the bank is not using cybersecurity policy.

	C	*A*	*M*	*E*	*L*	*CYBERSECURITY*
Mean	0.102445	0.011818	3.097518	10.01156	24.24802	0.6875
Standard Error	0.000564	0.00069	0.020485	0.101403	0.211366	0.008638544
Median	0.100956	0.006382	3.290407	9.579437	22.57913	1
Standard Deviation	0.03027	0.037028	1.099334	5.441831	11.3431	0.463592897
Sample Variance	0.000916	0.001371	1.208535	29.61352	128.666	0.214918374
Range	0.307482	0.702408	9.089	157.979	82.94993	1
Minimum	0.021604	0	-0.70902	-51.0793	1.353316	0
Maximum	0.329086	0.702408	8.379976	106.8996	84.30324	1

Table 6: Descriptive statistics of all bankrupt banks found in both files.

This table shows the descriptive statistics of all the factors of the CAMEL Model and cybersecurity variable of all the available bankrupted banks found in both files. C is the variable of Capital adequacy and is the Total Equity / Total Assets, A is the Asset quality and is the non-performing loans (NPLs)/ Assets, M is the Management and is the Net Interest Margin, E is the Earnings and is the ROAE, L is the Liquidity and is the Liquid Assets / Assets. Cybersecurity is binary and has the value of 1 if the bank is using policy on cybersecurity in place to protect from cyber-attack, unauthorized access, and data leaks and the value of 0 if the bank is not using cybersecurity policy..

	C	*A*	*M*	*E*	*L*	*CYBERSECURITY*
Mean	0.097849	0.013504	3.245832	10.51905	23.88186	0.866666667
Standard Error	0.001915	0.001114	0.098684	0.38978	0.80332	0.02784853
Median	0.096639	0.008254	3.215328	10.7863	23.23563	1
Standard Deviation	0.02345	0.013647	1.208622	4.77381	9.838618	0.341073447
Sample Variance	0.00055	0.000186	1.460767	22.78926	96.7984	0.116331096
Range	0.144275	0.077867	6.929096	38.68288	54.64487	1
Minimum	0.035958	0.000353	0.890892	-15.6911	2.564625	0
Maximum	0.180234	0.078221	7.819987	22.99175	57.2095	1

Table 7: Descriptive statistics of all sample

This table shows the descriptive statistics of all the factors of the CAMEL Model and cybersecurity variable of all the available healthy and bankrupted banks found in both files. C is the variable of Capital adequacy and is the Total Equity / Total Assets, A is the Asset quality and is the non-performing loans (NPLs)/ Assets, M is the Management and is the Net Interest Margin, E is the Earnings and is the ROAE, L is the Liquidity and is the Liquid Assets / Assets. Cybersecurity is binary and has the value of 1 if the bank is using policy on cybersecurity in place to protect from cyber-attack, unauthorized access, and data leaks and the value of 0 if the bank is not using cybersecurity policy.

b/h	*C*	*A*	*M*	*E*	*L*	*CYBERSECURITY*
Mean	0.102217	0.011901	3.10486	10.03668	24.2299	0.696369637
Standard Error	0.000545	0.000658	0.020079	0.098303	0.20478	0.008354931
Median	0.100586	0.006453	3.284455	9.65603	22.62758	1
Standard Deviation	0.029983	0.036228	1.105251	5.411116	11.27219	0.459900827
Sample Variance	0.000899	0.001312	1.221579	29.28017	127.0623	0.211508771
Range	0.307482	0.702408	9.089	157.979	82.94993	1
Minimum	0.021604	0	-0.70902	-51.0793	1.353316	0
Maximum	0.329086	0.702408	8.379976	106.8996	84.30324	1

Table 8: Correlation test of pairs (15 bankrupt and 15 healthy banks)

This table shows the correlation of all the factors of the CAMEL Model and cybersecurity variable of the paired sample which includes 15 bankrupted banks and 15 healthy.. C is the variable of Capital adequacy and is the Total Equity / Total Assets, A is the Asset quality and is the non-performing loans (NPLs)/ Assets, M is the Management and is the Net Interest Margin, E is the Earnings and is the ROAE, L is the Liquidity and is the Liquid Assets / Assets. Cybersecurity is binary and has the value of 1 if the bank is using policy on cybersecurity in place to protect from cyber-attack, unauthorized access, and data leaks and the value of 0 if the bank is not using cybersecurity policy..

	C	*A*	*M*	*E*	*L*	*CYBERSECURITY*
C	1					
A	0.145588	1				
M	0.489199	0.142931	1			
E	-0.01268	0.082986	0.479543	1		
L	0.094757	0.033432	-0.10369	-0.23789	1	
CYBERSECURITY	0.435752	0.121647	0.1265	-0.19699	-0.21105	1

Table 9: Correlation of all healthy banks found in both files

This table shows the correlation of all the factors of the CAMEL Model and cybersecurity variable of all the available healthy banks found in both files. C is the variable of Capital adequacy and is the Total Equity / Total Assets, A is the Asset quality and is the non-performing loans (NPLs)/ Assets, M is the Management and is the Net Interest Margin, E is the Earnings and is the ROAE, L is the Liquidity and is the Liquid Assets / Assets. Cybersecurity is binary and has the value of 1 if the bank is using policy on cybersecurity in place to protect from cyber-attack, unauthorized access, and data leaks and the value of 0 if the bank is not using cybersecurity policy..

	C	*A*	*M*	*E*	*L*	*CYBERSECURITY*
C	1					
A	0.13306	1				
M	0.440715	0.023103	1			
E	-0.09291	-0.08695	0.216043	1		
L	-0.1383	0.081941	-0.36978	-0.02794	1	
CYBERSECURITY	0.007449	0.037318	0.140991	0.046269	-0.0154	1

Table 10: Correlation of all bankrupt banks found in both files

This table shows the correlation of all the factors of the CAMEL Model and cybersecurity variable of all the available bankrupted banks found in both files. C is the variable of Capital adequacy and is the Total Equity / Total Assets, A is the Asset quality and is the non-performing loans (NPLs)/ Assets, M is the Management and is the Net Interest Margin, E is the Earnings and is the ROAE, L is the Liquidity and is the Liquid Assets / Assets. Cybersecurity is binary and has the value of 1 if the bank is using policy on cybersecurity in place to protect from cyber-attack, unauthorized access, and data leaks and the value of 0 if the bank is not using cybersecurity policy..

	C	*A*	*M*	*E*	*L*	*CYBERSECURITY*
C	1					
A	0.202358	1				
M	0.561329	-0.10519	1			
E	-0.31431	-0.28136	0.214825	1		
L	0.097191	0.348833	0.345945	0.148159	1	
CYBERSECURITY	0.13477	-0.04578	0.168086	-0.26175	-0.18306	1

Table 11: Correlation of all sample

This table shows the correlation of all the factors of the CAMEL Model and cybersecurity variable of all the available healthy and bankrupted banks found in both files. C is the variable of Capital adequacy and is the Total Equity / Total Assets, A is the Asset quality and is the non-performing loans (NPLs)/ Assets, M is the Management and is the Net Interest Margin, E is the Earnings and is the ROAE, L is the Liquidity and is the Liquid Assets / Assets. Cybersecurity is binary and has the value of 1 if the bank is using policy on cybersecurity in place to protect from cyber-attack, unauthorized access, and data leaks and the value of 0 if the bank is not using cybersecurity policy..

	C	*A*	*M*	*E*	*L*	*CYBERSECURITY*
C	1					
A	0.1331	1				
M	0.443293	0.020486	1			
E	-0.10101	-0.08934	0.216191	1		
L	-0.13005	0.085674	-0.33575	-0.0214	1	
CYBERSECURITY	0.008241	0.036768	0.143528	0.037878	-0.02127	1

Table 12: Test of differences in mean of the pairs

This tables presents the test of differences of mean of bankrupted and healthy banks in pairs of 15 bankrupted and 15 healthy banks.. C is the variable of Capital adequacy and is the Total Equity / Total Assets.

t-Test: Paired Two Sample for Means

	C	*C*
Mean	0.10230747	0.102847362
Variance	0.000298755	0.000683693
Observations	15	15
Pearson Correlation	0.143068221	
Hypothesized Mean Difference	0	
df	14	
t Stat	-0.071588724	
P(T<=t) one-tail	0.471970928	
t Critical one-tail	1.761310136	
P(T<=t) two-tail	0.943941856	
t Critical two-tail	2.144786688	

Table 13: Test of differences in mean of the pairs

This tables presents the test of differences of mean of bankrupted and healthy banks in pairs of 15 bankrupted and 15 healthy banks.. A is the Asset quality

t-Test: Paired Two Sample for Means

	A	*A*
Mean	0.051817912	0.014462101
Variance	0.018542785	0.000194949
Observations	15	15
Pearson Correlation	0.259937797	
Hypothesized Mean Difference	0	
df	14	
t Stat	1.085958401	
P(T<=t) one-tail	0.147921373	
t Critical one-tail	1.761310136	
P(T<=t) two-tail	0.295842746	
t Critical two-tail	2.144786688	

Table 14: Test of differences in mean of the pairs

This tables presents the test of differences of mean of bankrupted and healthy banks in pairs of 15 bankrupted and 15 healthy banks. M is the Management and is the Net Interest Margin

t-Test: Paired Two Sample for Means

	M	*M*
Mean	3.076914239	3.296310776
Variance	0.604052936	1.460710593
Observations	15	15
Pearson Correlation	0.11523902	
Hypothesized Mean Difference	0	
df	14	
t Stat	-0.6250186	
P(T<=t) one-tail	0.271006329	
t Critical one-tail	1.761310136	
P(T<=t) two-tail	0.542012657	
t Critical two-tail	2.144786688	

Table 15: Test of differences in mean of the pairs

This tables presents the test of differences of mean of bankrupted and healthy banks in pairs of 15 bankrupted and 15 healthy banks.. E is the Earnings and is the ROAE,

t-Test: Paired Two Sample for Means

	E	*E*
Mean	8.983403763	10.20070607
Variance	14.24144881	17.61882607
Observations	15	15
Pearson Correlation	-0.287258772	
Hypothesized Mean Difference	0	
df	14	

t Stat	-0.736647283
P(T<=t) one-tail	0.236750622
t Critical one-tail	1.761310136
P(T<=t) two-tail	0.473501243
t Critical two-tail	2.144786688

Table 16: Test of differences in mean of the pairs

This tables presents the test of differences of mean of bankrupted and healthy banks in pairs of 15 bankrupted and 15 healthy banks.. L is the Liquidity and is the Liquid Assets / Assets

t-Test: Paired Two Sample for Means

	L	*L*
Mean	30.43505	23.94135
Variance	134.5537	75.41366
Observations	15	15
Pearson Correlation	-0.19753	
Hypothesized Mean Difference	0	
df	14	
t Stat	1.59138	
P(T<=t) one-tail	0.066923	
t Critical one-tail	1.76131	
P(T<=t) two-tail	0.133845	
t Critical two-tail	2.144787	

Table 17: Test of differences in mean of the pairs

This tables presents the test of differences of mean of bankrupted and healthy banks in pairs of 15 bankrupted and 15 healthy banks Cybersecurity is binary and has the value of 1 if the bank is using policy on cybersecurity in place to protect from cyber-attack, unauthorized access, and data leaks and the value of 0 if the bank is not using cybersecurity policy..

t-Test: Paired Two Sample for Means

	cybersecurity policy	*cybersecurity policy*
Mean	0.466666667	0.533333333
Variance	0.266666667	0.266666667
Observations	15	15
Pearson Correlation	0.607142857	
Hypothesized Mean Difference	0	
df	14	
t Stat	-0.56407607	
P(T<=t) one-tail	0.290813418	
t Critical one-tail	1.761310136	
P(T<=t) two-tail	0.581626837	
t Critical two-tail	2.144786688	

Table 18: Test of differences in mean of all the sample

This tables presents the test of differences of mean of all bankrupted and healthy banks.. C is the variable of Capital adequacy and is the Total Equity / Total Assets

t-Test: Two-Sample Assuming Unequal Variances

	C	*C*
Mean	0.097849087	0.102444542
Variance	0.000549882	0.000916284
Observations	150	2880
Hypothesized Mean Difference	0	
df	176	
t Stat	-2.302327227	
P(T<=t) one-tail	0.011243682	
t Critical one-tail	1.653557435	
P(T<=t) two-tail	0.022487364	
t Critical two-tail	1.973534388	

Table 19: Test of differences in mean of all the sample

This tables presents the test of differences of mean of all bankrupted and healthy banks.. A is the Asset quality and is the non-performing loans (NPLs)/ Assets

t-Test: Two-Sample Assuming Unequal Variances

	A	*A*
Mean	0.013504	0.011817544
Variance	0.000186	0.001371082
Observations	150	2880
Hypothesized Mean Difference	0	
df	283	
t Stat	1.286492	
P(T<=t) one-tail	0.099661	
t Critical one-tail	1.650256	
P(T<=t) two-tail	0.199323	
t Critical two-tail	1.968382	

Table 20: Test of differences in mean of all the sample

This tables presents the test of differences of mean of all bankrupted and healthy banks.. M is the Management and is the Net Interest Margin

t-Test: Two-Sample Assuming Unequal Variances

	M	*M*
Mean	3.245832	3.097518
Variance	1.460767	1.208535
Observations	150	2880
Hypothesized Mean Difference	0	
df	162	
t Stat	1.471562	
P(T<=t) one-tail	0.071539	
t Critical one-tail	1.654314	
P(T<=t) two-tail	0.143079	
t Critical two-tail	1.974716	

Table 21: Test of differences in mean of all the sample

This tables presents the test of differences of mean of all bankrupted and healthy banks..E is the Earnings and is the ROAE

t-Test: Two-Sample Assuming Unequal Variances

	E	*E*
Mean	10.51904772	10.01155749
Variance	22.78926457	29.61351946
Observations	150	2880
Hypothesized Mean Difference	0	
df	170	
t Stat	1.260049664	
P(T<=t) one-tail	0.104689207	
t Critical one-tail	1.653866317	
P(T<=t) two-tail	0.209378413	
t Critical two-tail	1.974016708	

Table 22: Test of differences in mean of all the sample

This tables presents the test of differences of mean of all bankrupted and healthy banks.. L is the Liquidity and is the Liquid Assets / Assets.

t-Test: Two-Sample Assuming Unequal Variances

	L	*L*
Mean	23.88186	24.24802317
Variance	96.7984	128.6660238
Observations	150	2880
Hypothesized Mean Difference	0	
df	170	
t Stat	-0.44081	
P(T<=t) one-tail	0.329954	
t Critical one-tail	1.653866	
P(T<=t) two-tail	0.659909	
t Critical two-tail	1.974017	

Table 23: Test of differences in mean of all the sample

This tables presents the test of differences of mean of all bankrupted and healthy banks... Cybersecurity is binary and has the value of 1 if the bank is using policy on cybersecurity in place to protect from cyber-attack, unauthorized access, and data leaks and the value of 0 if the bank is not using cybersecurity policy..

t-Test: Two-Sample Assuming Unequal Variances

	CYBERSECURITY	*CYBERSECURITY*
Mean	0.866667	0.6875
Variance	0.116331	0.214918
Observations	150	2880
Hypothesized Mean Difference	0	
df	179	
t Stat	6.144769	
P(T<=t) one-tail	2.53E-09	
t Critical one-tail	1.653411	
P(T<=t) two-tail	5.06E-09	
t Critical two-tail	1.973305	

Table 24: Logistic regression model summary & Estimators of the Logistic Regression of the paired sample.

*This table shows the estimators of the logistic regression of the factors of the CAMEL Model and the cybersecurity variable of the paired sample. The binary variable who takes the value of 1 if the bank is defuncted (defaulted) and the value of zero if the bank is still operating (healthy). C is the variable of Capital adequacy and is the Total Equity / Total Assets, A is the Asset quality and is the non-performing loans (NPLs)/ Assets, M is the Management and is the Net Interest Margin, E is the Earnings and is the ROAE, L is the Liquidity and is the Liquid Assets / Assets. All these variables were collected from the S&P Market Intelligence Platform. Cybersecurity variable is binary and has the value of 1 if the bank is using and the value of zero if the bank is not using cybersecurity policies. Data for this variable collected from the UCY databases after communication with the relevant department and the professor in charge mr. Marios Kyriakou. Significance level of *,** and *** denotes two tail statistical significance of 10%, 5% and 1% respectively.*

Model Summary

Step	-2Log likelihood	Cox & Snell R Square	Nagelkerke R Square
1	38,379[a]	0,159	,213

Variables in the Equation	B	S.E.	Wald	df	Sig.	Exp(B)
C	-5.136	24.245	0.045	1	0.832	0.006
A	6.583	7.399	0.791	1	0.374	722.372
M	-0.067	0.530	0.016	1	0.899	0.935
E	-0.068	0.128	0.283	1	0.595	0.934
L	0.072	0.052	1.904		0.168	1.075
CYBERSECURITY	-0.195	0.954	0.042	1	0.038	0.823
Constant	-0.622	2.450	0.064	1	0.800	0.537

Table 25: Logistic regression model summary & Estimators of the Logistic Regression of all sample

*This table shows the estimators of the logistic regression of all the factors of the CAMEL Model and the cybersecurity variable. . The binary variable who takes the value of 1 if the bank is defuncted (defaulted) and the value of zero if the bank is still operating (healthy). C is the variable of Capital adequacy and is the Total Equity / Total Assets, A is the Asset quality and is the non-performing loans (NPLs)/ Assets, M is the Management and is the Net Interest Margin, E is the Earnings and is the ROAE, L is the Liquidity and is the Liquid Assets / Assets. All these variables were collected from the S&P Market Intelligence Platform. Cybersecurity variable is binary and has the value of 1 if the bank is using and the value of zero if the bank is not using cybersecurity policies. Data for this variable collected from the UCY databases after communication with the relevant department and the professor in charge mr. Marios Kyriakou. Significance level of *,** and *** denotes two tail statistical significance of 10%, 5% and 1% respectively.*

Model Summary

Step	-2Log likelihood	Cox & Snell R Square	Nagelkerke R Square
1	1159,761[a]	0.011	0.035

Variables in the Equation	B	S.E.	Wald	df	Sig.	Exp(B)
C	-10.467	3.945	7.040	1	0.008	0.000
A	1.564	1.877	0.695	1	0.405	4.779
M	0.182	0.093	3.835	1	0.050	1.199
E	0.001	0.017	0.002	1	0.965	1.001
L	-0.003	0.008	0.123	1	0.726	0.997
CYBERSECURITY	1.038	0.246	17.881	1	0.000	2.824
Constant	-3.259	0.518	39.562	1	0.000	0.038

Table 26: 1) Comparison of major research studies

Authors	Year	Dataset Period	Country	Data Sources	Research Question/Hypothesis	Dependent Variable(s)	Major Independent Variables	Major Conclusions
Akerlof, G. A.	1970	N/A	N/A	The Quarterly Journal of Economics	Examining market mechanisms with quality uncertainty.	Market Functioning	Information Asymmetry	Highlighted the importance of information in market quality.
Arner, D. W., et al.	2016	Post-Crisis	Global	Georgetown Journal of International Law	Discussing the evolution of FinTech post-crisis.	Financial Technology Evolution	Regulatory changes, Technological advancements	Identified the new paradigm of FinTech in the post-crisis era.
Basel Committee on Banking Supervision	2010	Post-Crisis	Global	Bank for International Settlements	Outlining the Net Stable Funding Ratio under Basel III.	Bank Regulation	Liquidity and Funding Requirements	Emphasized the need for stable funding to manage liquidity under cyber risks.
Biener, C., et al.	2015	N/A	N/A	The Geneva Papers on Risk and Insurance - Issues and Practice	Analyzing the insurability of cyber risk.	Cyber Risk Insurability	Cyber Incidents, Insurance Coverage	Quantified the impact of cyber incidents on financials.
Böhme, R., & Kataria, G.	2006	N/A	N/A	Workshop on the Economics of Information Security	Discussing correlation models in cyber-insurance.	Cyber-Insurance	Cyber Risk Correlation	Suggested models for understanding cyber-insurance economics.

Authors	Year	Dataset Period	Country	Data Sources	Research Question/Hypothesis	Dependent Variable(s)	Major Independent Variables	Major Conclusions
Charitou, S	2005	N/A	US	Regulatory filings, financial statements, and supervisory data provided by regulatory agencies like the Federal Reserve and the Federal Deposit Insurance Corporation (FDIC)	The significance of the new performance measures recommended by the Basel Accord on Banking Supervision, specifically assessing whether these measures are more important in explaining bank default compared to previous measures, and if the updated CAMELS Model incorporating these variables yields greater prediction accuracy.	The probability of default among US banks.	Capital adequacy, liquidity, and earnings, as suggested by the Basel Accord on Banking Supervision.	The inclusion of new performance measures recommended by the Basel Accord significantly improves the prediction of default probabilities among US banks, highlighting the importance of regulatory compliance for enhancing financial stability.
Darrat, A. F., et al.	2016	N/A	N/A	Journal of Accounting, Auditing & Finance	Exploring the impact of corporate governance on bankruptcy risk.	Bankruptcy Risk	Corporate Governance Metrics	Linked corporate governance quality with bankruptcy likelihood.
Demirgüç-Kunt, A., et al.	2013	Financial Crisis	Global	Journal of Money, Credit and Banking	Studying bank capital lessons from the financial crisis.	Bank Capital	Financial Indicators	Provided insights on bank capital adequacy during financial distress.
Eling, M., & Schnell, W.	2016	N/A	N/A	The Journal of Risk Finance	Surveying knowledge on cyber risk and cyber risk insurance.	Cyber Risk and Insurance	Cyber Incidents, Insurance Models	Reviewed the rising importance of cyber risk management.
Gordon, L. A., & Loeb, M. P.	2002	N/A	N/A	ACM Transactions on Information and System Security	Analyzing the economics of information security investment.	Information Security Investment	Cybersecurity Spending, Information Protection	Proposed an optimal investment model for information security.

Authors	Year	Dataset Period	Country	Data Sources	Research Question/Hypothesis	Dependent Variable(s)	Major Independent Variables	Major Conclusions
Jordan, D. J., Rice, D., Sanchez, J., Walker, C., & Wort, D. H.	2010	2007-2010	N/A	Regulatory filings, Financial statements, Economic and financial databases	The seven variables identified can be used to predict bank failure up to four years prior to the failure date. The ratio of the expense provision for bad debts as a percentage of total gross loans is a predictor of bank failure. The ratio of real estate loans as a percentage of total assets is a predictor of bank failure.	Whether a bank experienced failure during the period under investigation	Various financial metrics and indicators commonly used to assess the health and stability of banks.	The result shows that the model successfully predicts from 66.0%(4 years prior to failure)to 88.2%(1 year prior to failure)of failed banks, with an overall success rate of 76.8%. From the overall models, only Hypothesis 1&3 are accepted and hypothesis 2 is not rejected.
Romanosky, S.	2016	N/A	N/A	Journal of Cybersecurity	Examining costs and causes of cyber incidents.	Cyber Incidents	Financial Impact of Cyber Incidents	Highlighted financial implications of cybersecurity breaches.