Kasetsart Journal of Social Sciences 45 (2024) 901–914

Kasetsart Journal of Social Sciences

journal homepage: http://kjss.kasetsart.org

Financial resilience in ASEAN-4 banking sector: Impact of cyber risk disclosure

Etikah Karyani[a,*], Taufik Faturohman[b,†], Ana Noveria[b,†], Raden Aswin Rahadi[b,†]

[a] *Faculty of Economics and Business, Sebelas Maret University, Surakarta Town, Central Java 57126, Indonesia*
[b] *The School of Business and Management, Institute of Technology Bandung, Bandung 40132, Indonesia*

Article Info

Article history:
Received 26 May 2023
Revised 11 October 2023
Accepted 24 October 2023
Available online 30 August 2024

Keywords:
causes,
cyber risk disclosure,
financial resilience,
impacts,
risk governance

Abstract

The increasing complexity and digitalization of the banking industry has the potential for cyber risks that can disrupt banking performance. This study aims to investigate whether voluntary Cyber Risk Disclosure (VCRD) influences banks' financial resilience. This study, to the researcher's knowledge, is a preliminary study that analyzes VCRD and financial resilience in ASEAN-4 financial industry. The sample used consisted of 310 observations from 62 banks listed on the Indonesia, Malaysia, Thailand, and the Philippines Stock Exchanges during the 2015–2020 period. Voluntary CRD are proxied by the governance, causes and impacts of cyber risk. The study result shows that total and individual voluntary CRD reduces bank resilience unless the causes of cyber risk does not affect it. These results remain unchanged after examining a robustness test. The implications of this finding are ASEAN-4 financial regulators should continue to put more pressure on disclosure of cyber threats as "events like this are important to the market". However, disclosure can weaken the financial resilience of banks so that the cooperation of many parties is needed and regulatory intervention is very important.

* Corresponding author.
E-mail address: etikah.karyani@staff.uns.ac.id (E. Karyani).
† Co-first authors.
E-mail address: taufik.f@sbm-itb.ac.id (T. Faturohman).
E-mail address: ana.noveria@sbm-itb.ac.id (A. Noveria).
E-mail address: aswin.rahadi@sbm-itb.ac.id (R. A. Rahadi).

https://doi.org/10.34044/j.kjss.2024.45.3.20
2452–3151/© 2024 Kasetsart University.

Introduction

The COVID-19 pandemic was an exogenous shock and banks contributed substantially to supporting emergency responses around the world. Banks are required to assist especially financial regulators and supervisors in maintaining financial stability. On the one hand, this crisis proved that banks were recognized as more resilient than in the 2008 crisis with more capital and better liquidity (KPMG, 2020). On the other hand, as the pandemic developed, with no end in sight, with banks still having to continue to face challenges to maintain profitability and future financial resilience, banks also faced potential losses due to cyber breaches. The 2021 COVID crime index study reported that cyber crime was the main factor that hindered or affected financial institutions and their customers during the previous 12 months (March 2020 to March 2021). The index found that 56 percent of US and UK banks and insurance companies experienced an increase in financial losses and such continued to increase. Furthermore, on average, budgets in information technology (IT) security, cybercrime, fraud, and risk departments were cut 26 percent to 36 percent, and they had to reduce the number of people on the IT security team.

Therefore, cyber risk presents a corporate governance challenge for these institutions to manage, as well as a threat to financial stability and resilience that bank regulators must address. Among financial regulators, the US Securities and Exchange Commission ("SEC") pays close attention to cyber risk. While the SEC has taken several steps forward, banking laws and regulations particularly in Asia emerging countries have remained relatively sluggish in the face of increasing cyber risks. Meanwhile, since the global financial crisis of 2008/09, there have been growing concerns about the resilience of the banking system in Southeast Asia. Since the pandemic, regulators in the region have refocused the issue of resilience on financial institutions, for example the Asian Development Bank (ADB) together with AMRO assessed major economic and financial developments since the Asian financial crisis (ADB, 2021). In addition, it is necessary to study financial resilience and its factors in relation to the development of disruptive technology (Brusset & Teller, 2017).

Therefore, this study examined whether the financial resilience of ASEAN banks related to the increasing reported cyber risk issues. Our study contributes to the literature on cyber security issues and cyber business ethics that was expected to contribute by filling the previous research gap. First, according to the researcher's knowledge, this is the first study linking financial resilience and operational resilience (cyber risk) which is voluntarily disclosed in the banking annual report. Previous studies have focused more on macroeconomic variables as the cause of banking financial resilience (for example Albert & Hee Ng, 2012; Cecchetti & Tucker, 2016; Ruza et al., 2019). We focused on financial resilience in measuring banking performance because many new products and services have been born due to the development of internet technology which has shifted conventional services so that there is a need for a study related to financial resilience and its factors (Brusset & Teller, 2017). Moreover, since the pandemic, banks are required to have financial resilience because regulators are worried about the bank's response to such rapid changes (KPMG, 2020).

Second, previous studies have shown mixed and limited results regarding the consequences of voluntary risk disclosure. In the context of disclosures that cover cybersecurity issues, Campbell et al. (2014) documented the market reaction to the disclosure of unexpected risk factors, and Hope et al. (2016) found the market reacted positively to the disclosure of more specific risk factors. In contrast, the informativeness of disclosure of cyber risk factors has negative consequences (for example Kamiya et al., 2021). Arguably, there is little empirical work on disclosure of voluntary operational risk in general and bank resilience. Such studies also examine risk factor disclosure less at the individual level than at the aggregate level (Li et al, 2018). In addition, there is a contextual gap in this regard; most of the empirical research related to this is carried out in developed countries using related settings there, while the phenomenon is widespread. Therefore, there is a need to investigate this aspect in a developing region such as Asia, placing particular emphasis on ASEAN banking. This research will help enrich the literature in the field of voluntary disclosure of information in the banking industry.

Finally, it is important to use a sample of ASEAN banks as regulators in the region developing the ASEAN Digital Masterplan (ADM) 2025 to support Cyber security to fulfill ASEAN Digital Ambition. ASEAN is a region that was already experiencing accelerated digitisation before the COVID-19 outbreak and such accelerated further during the pandemic. In addition, ASEAN is one of the world's fastest growing internet markets with 125,000 new users logging on to the internet every day. Therefore, cyber security is crucial to face the increasingly complex challenges of cybercrime in the future. To achieve this goal, the manuscript hand-collected

and examined data on what is disclosed by commercial banks listed on four emerging market exchanges and four middle-income statuses of The Association of Southeast Asian Nations (ASEAN-4), namely, Indonesia, Malaysia, Thailand, and the Philippines regarding exposure to cyber risks.

Specifically, we hand collected three types of voluntary disclosure (risk governance, causes, and impacts) over a five-year span (2015–2020). Our findings on nearly 310 observations show new problems, such as the level of cyber risk disclosure both total and by specific disclosures of public companies, which is still very low. This proves that they do not reveal much about their exposure to cyber risk and do not disclose it adequately to the market. We also find that the resilience level is influenced by banks that are more disclosing about risk governance and the impact of cyber incidents, while it is not influenced by disclosures regarding the causes of their cyber risk which shows this type of disclosure is not informative. This result is robust when regressed with the estimate of Two Stage Least Square (2SLS).

This paper was divided into five sections to present the research approach. Section 2 is dedicated to the literature review. This study makes a case for applying the theory of financial resilience to develop a cybersecurity disclosure framework. Section 3 describe the data and methodology. In Section 4, the authors present a discussion based on the research work in Sections 1 to 4. Section 5 concludes the research paper.

Literature Review

Theory of Financial Resilience and Measuring Financial Resilience

Salter and Tarko (2017) developed a theory of financial resilience to better understand the causes of financial stability (and instability). Resilience is a property of the institutions that govern the life of a social system. Thus, financial resilience refers to the institutions that make the financial system stable. “Stability” is a firm’s ability to minimize the likelihood of balance sheet shocks leading to systemic bankruptcy and minimize the likelihood of such balance sheet shocks in the first place. Financial resilience was first defined by McDonough in 2003. Furthermore, O’Neill (2011) defines financial resilience as the ability to withstand life events that have an impact on one’s income and/or assets. Some financially stressful events, such as recessions, stock market declines, and acts of terrorism, affect society.

The concept of financial resilience has been studied from various dimensions, and the discussion on measuring financial resilience is focused on a quantification approach that uses components of a company’s financial performance. Existing quantitative methods usually divide companies into good and bad groups by classifying financial resilience. Previous studies measured financial resilience using key indicators including stock prices, income before interest and taxes, the ratio of total liabilities to the total value of company assets, working capital on total assets, and earnings per share (see Guettafi & Laib, 2016; Hallegatte, 2014; Nkundabanyanga et al., 2020; Soufi et al., 2023; Triggs et al., 2019). Other literature (see Maheswaran & Rao, 2014; Patra & Padhi, 2020; Ghosh & Saima, 2021) used capital adequacy, liquidity ratios, and non-performing loans (NPL) to measure the resilience of financial institutions. Risk-based financial resilience measures are Value at Risk (VaR) and Conditional Value at Risk (CoVaR) (Soufi et al., 2023) and stress testing to estimate the impact of macroeconomic shocks on NPL ratios and minimum capital evaluation (Albert & Hee Ng, 2012). In addition, bank resilience is measured by a composite indicator (CI) to predict future bank behavior (Cecchetti & Tucker, 2016; Ruza et al., 2019) and a system resilience index that includes transparency and accounting variables (Guettafi & Laib, 2016).

VCRD and Financial Resilience (FR)

As of March 2022, US listed companies were required to increase disclosure about corporate governance, risk management, and strategies related to cybersecurity risks. Details on disclosure include management and board roles and cybersecurity risk oversight; cyber security policies and procedures; and cybersecurity risks and incidents likely impact company finance. Most of the motives of cyber criminals are carried out through phishing, ransonware, and malware. The consequences of cyberattacks can lead to financial losses and loss of customers (Tariq, 2018). This fact is supported by Fortunly’s assessment that the cost of cyberattacks in the banking industry has reached $18.3 million per year per company, which results in financial losses and erodes user confidence. Research from the Bank of England’s 2022 Systemic Risk Survey also shows that 74 percent of respondents consider cyberattacks to be the highest risk to the financial sector. Furthermore, the failures of financial institutions are due to weak risk governance and insufficient disclosure and transparency in reporting, and inadequate risk management frameworks to identify, measure, and control the risks associated with their activities (Karyani et al., 2019; 2020; 2021).

Meanwhile, doubts regarding the informativeness of risk factor disclosure remain debatable. On the one stream, previous research shows that disclosure of cyber risk or IT risk provides investor with the useful information and improves stock performance (Histen, 2022). Berkman et al. (2018) found that proactive voluntary disclosure of information security in annual reports shows a positive relationship with stock prices. Agency theory suggests that better disclosure can reduce information asymmetry between management and investors, reduce the cost of capital, and thus improve the liquidity of companies and their access to capital markets. In an information asymmetric environment, investors realise that management may take advantage of their position by issuing securities at a higher price. As a result, investors demand a discount to compensate for the risk of adverse selection in the form of a higher cost of capital (see Leuz & Wysocki, 2016). In other words, when firms provide more disclosures, the risk of adverse selection can be reduced, which ultimately lowers the firm's cost of capital and increases the firm's financial resilience value. In addition, greater cyber disclosure demonstrates the accountability of managers and board members for adequate cyber risk management (Skinner, 2019). Berkman et al. (2018) found companies that disclose proactive security activities and demonstrate cybersecurity awareness have higher market valuations.

Otherwise, another stream of research provides ample evidence of the negative market and economic consequences of cyber incidents. According to Skinner (2019), systemically banks can present a special case when publishing details of a bank's cyber vulnerabilities as it can further weaken the bank and cause macro-instability. Information about a cyber breach in a large bank can trigger panic in depositors, thereby accelerating the perceived decline in the value of the bank's assets. However, upon discovery of a breach, investors reassess the distribution of losses from the breached company's cybersecurity risk and react negatively, especially when the breach is severe (Kamiya et al., 2021).

Based on the arguments above, we developed a non-direction hypothesis for banks that disclose overall cyber risk, cyber risk governance, cause and impact of cyber risk.

Hyp1: Overall voluntary cyber risk disclosure affects bank financial resilience

Hyp2: Disclosure of the cyber risk governance affects bank financial resilience

Hyp3: Disclosure of the causes of cyber risk affects bank financial resilience

Hyp4: Disclosure of the impacts of cyber risk affects bank financial resilience

Methodology

Sample Selection and Data Collection

The purpose of this study is to examine how voluntary disclosure of cyber risk affects financial resilience. Our sample includes 67 commercial banks listed in four ASEAN countries: Indonesia (27 banks), Malaysia (5 banks), Thailand (11 banks), and the Philippines (14 banks). We have eliminated regional or rural Banks because these banks have less digital technology and therefore fewer cybersecurity threat. Our focus on listed commercial banks may be more digital and therefore fewer cybersecurity threats. These banks are also likely to be more widely disclosed to meet the needs of investors and regulators and more resilient to cyber shocks, in particular. From 2015 to 2020, the definitive sample included 310 bank-year observations. The information was gathered from the English version of the annual report, which can be found on the bank's official website, as well as BankFocus BvD.

Empirical Models and Variables description

The following is the definition of our empirical bank resilience models (Equation (1), (2), (3), and (4)):

$$\begin{aligned} LNFRit = {} & \alpha 0 + \alpha 1VCRDit + \alpha 5LNSIZEit + \\ & \alpha 6LEVit + \alpha 7NPL\ it + \alpha 8LDRit + \\ & \alpha 9GDPGit + \alpha 10VAit + \alpha 11PVit + \varepsilon it \quad (1) \end{aligned}$$

$$\begin{aligned} LNFRit = {} & \alpha 0 + \alpha 2GCRit + \alpha 5LNSIZEit + \\ & \alpha 6LEVit + \alpha 7NPL\ it + \alpha 8LDRit + \\ & \alpha 9GDPGit + \alpha 10VAit + \alpha 11PVit + \varepsilon it \quad (2) \end{aligned}$$

$$\begin{aligned} LNFRit = {} & \alpha 0 + \alpha 3CAUSESit + \alpha 5LNSIZEit + \\ & \alpha 6LEVit + \alpha 7NPL\ it + \alpha 8LDRit + \\ & \alpha 9GDPGit + \alpha 10VAit + \alpha 11PVit + \varepsilon it \quad (3) \end{aligned}$$

$$\begin{aligned} LNFRit = {} & \alpha 0 + \alpha 4IMPACTSit + \alpha 5LNSIZEit + \\ & \alpha 6LEVit + \alpha 7NPL\ it + \alpha 8LDRit + \\ & \alpha 9GDPGit + \alpha 10VAit + \alpha 11PVit + \varepsilon it \quad (4) \end{aligned}$$

Financial Resilience (LNFR)

This study employs the method developed by Vallascas and Keasey (2012) based on Merton's (1974) distance to default model or default beta (βDD) to measure the bank resilience (LNFR). Different from the approach to measuring bank resilience in general, we focused on the resilience of market-based finance which assesses activity and market due to limitations, and perceived market equity is more volatile. Compared to other indicators, such as accounting-based indicators,

market-based indicators have the advantage of providing a near real-time view as market prices reflect the changing expectations of market participants. Market-based indicators also tend to be more responsive to changes in banking system resilience.

Merton's (1974) distance to default model is used to estimate the default risk for the entire system or describe the sensitivity of a bank's default risk to systemic shocks and employed contingent claim analysis (CCA). By modeling bank equity as a call option on the market value of assets, the Distance to Default (DD) reflects the number of standard deviations that the market value of bank assets is above the default point. DD formula is as follows (Equation (5)):

$$DD_t = \left[\ln\left(\frac{V_{A,t}}{X_t}\right) + \left(r_f - 0.5\sigma_{A,t}^2\right)T\right] / \sigma_{A,t}\sqrt{T} \quad (5)$$

Where DD on day t is calculated based on the Merton credit risk model with VA,t as the market value of assets, Xt as the book value of total liabilities, rf as the risk-free rate (refer to the 12 month government bond rate), σA,t as the annualized asset volatility at t, and T as the time to maturity (generally set to 1 year). The market value of assets is obtained by multiplying the bank's outstanding shares by its respective stock price. The data are sourced from Quarterly Financial Report and trading economics.

The banking system default or distance to default index (IDD) is then calculated by averaging all distances to defaults measured on a quartal frequency and at the bank level. Aggregate series of distances to default are commonly used in policy reports on financial stability as an indicator of systemic risk, as used by the European Central Bank and IMF (European Central Bank, 2005; Vallascas, & Keasey, 2012). Then, the distance to default beta (βDD) as the bank resilience variable is obtained from the slope coefficient (beta) of the following regression model (Equation (6)):

$$\left(\frac{DD_t^i - DD_{t-1}^i}{\left|DD_{t-1}^i\right|}\right) = \alpha_0 + \beta_{DD_{i,t}}\left(\frac{IDD_t^i - IDD_{t-1}^i}{\left|IDD_{t-1}^i\right|}\right) + \varepsilon_{i,t} \quad (6)$$

Where $(DD_t^i - DD_{t-1}^i)/|DD_{t-1}^i|$ is the relative change of distance to default for bank i, $(IDD_t^i - IDD_{t-1}^i)/|IDD_{t-1}^i|$ is the relative change in the distance to default index, and is the residual, and $\varepsilon_{i,t}$ is the residual. According to Gropp and Moerman (2004), median regression is used to estimate the $\beta_{DD_{i,t}}$ in order to minimize the impact of outliers and to remove the distributional assumptions of traditional estimating methods. Therefore, $\beta_{DD_{i,t}}$, which in this study is used as a bank resilience variable, assesses how a bank's default risk responds to changes in banking system risk with higher absolute values signifying increased sensitivity to systemic shock.

Voluntary Cyber Risk Disclosure (VCRD)

The content analysis method was used to collect VCRD based on a rule proposed by the Securities and Exchange Commission ("SEC") in March 2022 that requires public companies to make cybersecurity disclosures (Gensler, 2022). We simplified these elements to fit the ASEAN banking practice of revealing cyber risk, which includes governance practices, as well as causes and implications of cyber risk. Governance of cyber risk (GCR) refers to whether the bank's board (discussion board) takes over cyber risk, any strategy/policy related to cyber risk management, the bank defines cyber risk clearly, and the bank identifies cyber risk as a material item. CAUSES describe the causes of cyber incidents including items, such as malware, phishing, trojans, ransomware, data breaches. Meantime, IMPACTS involve the damage to the bank reputation, financial losses, and legal actions or implications. These three elements represent the types of disclosure that are "organizational/neutral", "positive/preventive", and "negative/risk".

The VCRD index is calculated by dividing the number of items disclosed (n) by the number of things that should be reported (n) (k). The maximum score that can be obtained in the VCRD measurement is the total number of usage scores divided by the total disclosure items. The higher a bank's index score, the more items it has disclosed. Banks with a higher index score have more thorough disclosure policies. The validity and reliability tests were performed to determine whether the VCRD index was "good" or "adequate" based on a Cronbach's alpha value of .60–.70. (Clark & Watson, 1995).

Control Variables

Furthermore, the control variables were used based on the study of Ruza et al. (2019) which includes Bank's Asset Size (SIZE), Leverage (LEV), Non-Performing Loans (NPL), loan-to-deposit ratio (LDR), gross domestic product growth (GDPG) and country risk, proxied by voice and accountability (VA) and politic stability (PV) of International Country Risk Guide (ICRG). There is a consensus that large company size (SIZE) has a positive impact, but also a negative effect because it endangers the entire system or systemically. Banks with greater bank capital (LEV) are associated with higher bank values

and are more resilient in times of crisis. The decline in bank asset quality from non- performing loans (NPL) limited bank performance and economic recovery by absorbing higher losses as was the case in Asia of the late 1990s. Meanwhile, the resilience of the banking system in many OECD countries has been strengthened after the implementation of Basel III in accordance with higher minimum capital and liquidity requirements. Furthermore, Han and Melecky (2013) observed that countries with high and middle incomes have easier access to deposit ratios which increase the resilience of the funding base of the banking sector deposits. Finally, Huang and Lin (2021) stated that country risk reduces bank stability in both developed and developing countries.

This study uses the Two Stage Least Square (2SLS) approach to solve equations that do not produce unbiased exogenous variables. The first step is to regress the endogenous explanatory variables on instrumental variables and other exogenous variables. The second step is to regress the endogenous variable on the unbiased explanatory endogenous variable along with other variables. Furthermore, Additional analyses were conducted by testing with a different method, namely, the Ordinary Least Squares (OLS) approach. This test is also used to prove the effectiveness of the regression results and the robustness of the instrument variable estimators.

Results

Multivariate Analysis

Table 1 reports the descriptive statistics of the sample from 2015 to 2020 for the firm and country characteristics of our sample. We observed the main variable from the study that the average company has a not so high resilience of 3.4073 (less close to zero) with the highest average being Malaysian banking (1.9538) followed by Thai banking (2.9600), Philippines (3.1473) and Indonesia (3.6163).

Furthermore, ASEAN-4 banking experienced the biggest decline in resilience in 2019 as shown in Figure 1. According to OECD survey (2021), Asia Pacific experienced the sharpest decline in vulnerability throughout 2019, even lower than the 2007 crisis.

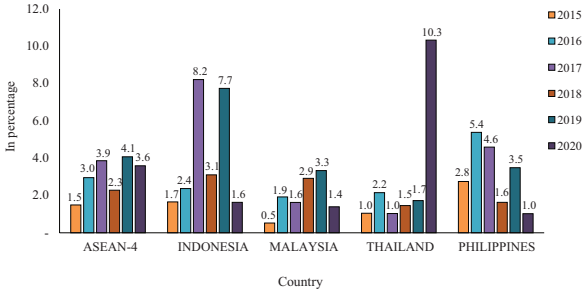

Figure 1 The mean of financial resilience of ASEAN-4 banks

Table 1 Summary of statistics

Variables	Mean	Min	Max	Median	Standard Deviation
FR	3.407328	0.009750	28.08430	1.970959	4.217781
VCRD	0.219355	0.000000	0.750000	0.166667	0.143485
GCR	0.540323	0.000000	1.000000	0.500000	0.277943
CAUSES	0.063594	0.000000	0.714286	0.000000	0.132686
IMPACTS	0.014516	0.000000	0.500000	0.000000	0.084084
lnSize	22.38524	18.09769	25.54294	22.48973	1.852112
Leverage	0.816032	0.030000	0.970000	0.860000	0.166308
NPL	0.030284	0.000000	0.158200	0.027400	0.020321
LDR	0.708822	0.000000	1.271387	0.730472	0.167189
GDPG	0.050897	0.022664	0.071495	0.050331	0.009823
VA	0.554839	0.375000	0.750000	0.541667	0.092261
PV	0.625477	0.560606	0.725379	0.617424	0.045390

Note: Financial resilience (FR): bank resilience, VCRD: cyber risk disclosure, GCR: governance of cyber risk, CAUSES: Cause of cyber risk, IMPACTS: Impact of cyber risk, Bank size (lnSIZE): natural logarithm of total assets, Leverage (LEV): Banks' Financial Assets/ Equity, Non-performing loans (NPL): Domestic Credit to the Private Sector/Banks' Total Assets, Loans deposits ratio (LDR): Total liabilities (−) Equity (−) Reserves (−) Derivatives (−) Funds from customers/GDP, Growth of gross domestic product (GDPG): Real growth of GDP, VA: country risk-political right, PV: country risk-political stability.

This indicates that the bank entered the crisis with less income to offset past losses (Moretti et al., 2020). Low interest margins could have been exacerbated by the low interest rate environment of monetary policy actions by major central banks since early 2020 (EBA, 2020). Thailand's banking system experienced the lowest resilience decline in 2020, that was influenced by a sudden cessation of tourism flows and a significant contraction during the pandemic (Kaendera & Leigh, 2021). Meanwhile, Malaysian banks have the best mean level of resilience compared to banks in the other three sample countries, at 2. In contrast to Malaysian banks, which have a persistent level of resilience over the study period, Philippine and Indonesian banks have a fluctuating level of resilience. However, in the year of the 2020 pandemic, Philippine banks had the strongest resilience level compared to the years before the pandemic, which was around 1. This is in accordance with the BIS study which states that a strong and resilient banking system is one of the drivers of the strong Philippine Peso currency, considered one of the strongest currencies in the region. Banks in Indonesia experienced low resilience (away from 0) in 2017 and 2019, at 8 and 7 respectively. Around 80–100 percent of corporate funding in Indonesia comes from bank loans, but lending and third party funds (DPK) of banks in 2017 and 2019 experienced a significant decline. This resulted in a decline in bank profitability and capitalisation.

Furthermore, Table 1 explains that the mean of cyber disclosure level (aggregate) in ASEAN-4 is only 21.9 percent. The number of disclosures of cybersecurity risk factors in all companies increased throughout the observation period. For the selected comparative analysis discussed in the next section, we examined the governance-related keyword list for a risk of 54.03 percent, the mean occurrence related to the cause of cyber risk is 6.35 percent, and the impact of cyber risk is only 1.45 percent. In general, it can be concluded that the level of cyber risk disclosure in ASEAN-4 banks is very low (< 50%) both in terms of disclosure related to the causes and consequences of cyber risk, except for disclosure of cyber risk governance. Our study is supported by the observations of Amir et al. (2018) on managers' decisions to withhold disclosure of incidents of cyber data breaches.

The control variables presented in Table 1 illustrate that ASEAN-4 banks had a mean value of asset of USD 20 billion (unlog 22.38), which is mostly owned by Malaysian and Thai banks. As measured by banks' financial assets/equity (Vallascas & Keasey, 2012; Ruza et al., 2019), ASEAN-4 banks had a mean value of leverage value of 81.6 percent. It illustrates the ability of banks to multiply and raise third-party funds from available equity which is quite high. Meanwhile, credit quality, proxied by the mean value of non-performing loans (NPL) (domestic credit to the private sector/banks' total assets), amounted to three percent. When compared to countries in the ASEAN-4 region, the mean NPL of banks in Malaysia is quite low (less than the mean NPL of ASEAN-4 banks). The mean value of liquidity or loans deposits ratio (LDR), as measured by Total liabilities (-) equity (-) reserves (-) derivatives (-) Funds from customers/GDP (OECD, 2021), is 70.88 percent. It describes the ability of ASEAN-4 banks to extend credit from collected third-party funds is below the ideal (75%–80%) to support economic growth and fulfill bank healt.

At the country level, the mean GDP growth (GGDP) of ASEAN-4 countries is 5.5 percent, which decreased significantly in 2020. According to Huang and Lin (2021), voice and accountability (VA) and political stability (PV) are country risk proxies. The mean value of VA and PV of ASEAN-4 countries is 55 percent and 62 percent respectively. Higher VA and PV performance scores (from 0 to 100) reflect the better the situation. Malaysia's mean VA and PV scores outperformed the other three countries.

Since the normality slope test showed that all predictive variables were not normally distributed, we performed a non-parametric Spearman rho correlation analysis, which is summarized in Table 2. The table reports the correlation matrix which contains the correlation coefficients between variables. The results of the correlation test show that there is no correlation between the independent variables with high and significant value, which indicates that there is no multicollinearity problem. The correlation coefficient only measures the strength of the linear relationship and not the non-linear relationship.

Furthermore, the regression results, which can explain the causality or causal relationship, are shown in Table 3. The relationship between resilience and VCRD (Hyp 1), GCR (Hyp 2), and IMPACT (hyp 4) is positive and significant as indicated by the coefficient values of 0.9147, 0.5054 and 1.8148 at the $p < .01$ level. That is, the more banks increase their overall disclosure of cyber risk, disclosure of governance and causes of cyber risk, the lower their financial resilience will be. In this case, the bank's resilience value is close to zero, the higher the resilience.

Table 2 Correlation matrix for outcome variables

Correlation Probability	CRD	GCR	CAUSES	IMPACTS	LNSIZE	LEV	NPL	LDR	VA	PV	GDPG
CRD	1.000000										

GCR	0.867928	1.000000									
	0.0000	-----									
CAUSES	0.800846	0.412881	1.000000								
	0.0000	0.0000	-----								
IMPACTS	0.104051	0.009492	-0.000134	1.000000							
	0.0673	0.8678	0.9981	-----							
LNSIZE	0.413411	0.454196	0.239814	-0.069441	1.000000						
	0.0000	0.0000	0.0000	0.2228	-----						
LEV	-0.000704	0.049855	-0.064580	0.024961	0.160103	1.000000					
	0.9901	0.3817	0.2569	0.6616	0.0047	-----					
NPL	-0.203677	-0.242183	-0.110647	0.119834	-0.286451	0.054525	1.000000				
	0.0003	0.0000	0.0516	0.0349	0.0000	0.3386	-----				
LDR	0.118471	0.163190	0.026495	-0.008684	0.322861	0.463050	-0.044957	1.000000			
	0.0371	0.0040	0.6422	0.8790	0.0000	0.0000	0.4303	-----			
VA	0.229219	0.122513	0.266523	0.062182	0.014638	0.169426	-0.135015	-0.141021	1.000000		
	0.0000	0.0310	0.0000	0.2751	0.7974	0.0028	0.0174	0.0129	-----		
PV	0.243176	0.136208	0.301137	-0.101388	0.291867	-0.093165	-0.125858	-0.134499	0.319032	1.000000	
	0.0000	0.0164	0.0000	0.0747	0.0000	0.1016	0.0267	0.0178	0.0000	-----	
GDPG	-0.039814	-0.133353	0.083439	0.008945	-0.167872	0.286220	-0.033063	-0.118012	0.606567	0.255068	1.000000
	0.4849	0.0188	0.1427	0.8754	0.0030	0.0000	0.5620	0.0378	0.0000	0.0000	-----

Table 3 Result of models (2SLS)

Variables	(1)	(2)	(3)	(4)
	VCRD	GCR	CAUSES	IMPACTS
	(SE)	(SE)	(SE)	(SE)
VCRD	0.9147 ***			
	(0.3292)			
GCR		0.5054 ***		
		(0.1809)		
CAUSESs			0.1430	
			(0.3275)	
IMPACTSs				1.8148 ***
				(0.5762)
Size	-0.0032	-0.0046	0.0211	0.0247
	(0.0359)	(0.0358)	(0.0347)	(0.0338)
Lev	0.8915 *	0.8239	0.8275 *	0.7956
	(0.5085)	(0.5062)	(0.5003)	(0.5030)
NPL	6.5032 **	7.4668 ***	6.7910 **	5.7256 **
	(2.7967)	(2.7589)	(2.6756)	(2.7589)
LDR	-0.6688 *	-0.6395 *	-0.6324 *	-0.5036
	(0.3685)	(0.3647)	(0.3648)	(0.4567)
GDPG	0.3512	0.3176	0.1869	0.2203
	(0.2563)	(0.2565)	(0.2603)	(0.2700)
VA	1.0356	1.3639 **	1.5966 **	1.5558 **
	(0.6751)	(0.6665)	(0.7085)	(0.7294)
PV	-4.6093 ***	-4.4632 ***	-4.5491	-3.7454 ***
	(1.2354)	(1.2045)	(1.2413)	(1.2320)
Observations	310	310	310	310
Adj. R-squared	0.1047	0.1098	0.0929	0.1139
Prob (*F*-statistic)	0.0000	0.0000	0.0000	0.0000

Meanwhile, the relationship between resilience and CAUSES (Hyp 3) is not significant with a coefficient of 0.1430 ($p < .01$, $p < .05$ and $p < .10$) as shown in Model 3. Adjusted R-squared (adj. R^2) values of the four models are 0.1047, 0.1098, 0.0929, and 0.1139. This shows that the four models each have variations of 10.47 percent, 10.98 percent, 9.29 percent and 11.39 percent to explain the effect of the independent variables on resilience (the dependent variable). The *p* values for the F-test for all models are significant, which provides evidence that the sample data are sufficient to conclude that this regression model is good.

Control variables that have a significant effect on resilience are SIZE (Model 3 and 4), LEV (Model 1 and 2), NPL (all models), VA (models 2, 3 and 4), and PV (models 1 and 2) at various levels ($p < .01$, $p < .05$ and $p < .10$). Significantly positive association between SIZE, LEV, NPL variables and the dependent variable explains the higher financial resilience when the banks size, leverage and non-performing loans are lower, while the different results at the country level are that the financial resilience variable is positively related to government accountability and negatively related to political stability. This means that the financial resilience of banks will be higher if government accountability is lower and the country's political conditions are more stable. On the other hand, the association between bank liquidity (LDR) and financial resilience is negative but not significant, while the relationship between GDPG and financial resilience of banks is positive and insignificant at the significance levels of 1 percent, 5 percent, and 10 percent.

Discussion

The study result shows that financial resilience decreases significantly if banks disclose the total and individual cyber risk (governance and impact of cyber risk events). This is consistent with the study by Chen et al. (2022), that the market anticipates increased disclosure after a data breach. Equity investors are aware of increased cybersecurity risks and react to disclosures resulting from cyber risks that occur to banks. Equity investors reacted negatively to data breach announcements, particularly to breaches involving unauthorized access to confidential data (Kamiya et al., 2021). Moreover, banks receive biased incentives when providing unfavorable information including concerns about the impact on firm valuation, cost of capital, debt contract negotiations, and executive compensation and career opportunities. It implies that risk disclosure is informative, at least as a predictor of future data breaches (Li et al., 2018).

In theory, informing the market through public disclosure of cyber security risks is considered a way to reduce information asymmetry and provide good signaling (Jiang et al., 2022). On the other hand, there are economic consequences of disclosing the governance and impact of cyber events. Companies increasingly making these disclosures are, in effect, also signaling concerns about cybersecurity (Havakhor et al., 2021). Therefore, if the market does not reward these disclosures, companies are still not incentivised and disclosure activities could potentially decrease company resilience.

There is no significant financial resilience if the next annual report of the violated company includes the causes of cybersecurity risk factors. This is consistent with the study by Hilary et al. (2016), who did not find a significant increase in the relationship between disclosure of security risks after a data breach. This implies that disclosure of the causes of cyber risk in the risk factors and MD&A sections is not informative. In addition, firms may simply disclose all possible risks using generic and repetitive (i.e., boilerplate) language (Beatty et al., 2019).

Furthermore, the findings from the regression results for the control variables indicate that high leverage and NPL reduce the bank's financial resilience. This implies that there is a need to be careful about risk exposure and protection from systemic shocks. Banks with higher leverage are also more prone to failure in the event of systemic events. Thus, limiting a bank's leverage ratio and imposing liquidity requirements, in accordance with Basel III regulations, can also increase a bank's resilience from systemic events (Vallascas & Keasey, 2012). Furthermore, a high level of bank liquidity encourages resilience. Budnik and Bochmann (2017) state that bank liquidity is aimed at reducing fluctuations in bank loans during the business cycle. The study by Buch et al. (2014) also supports that US banks with higher capital to liquidity ratios are less exposed to macroeconomic shocks. On the other hand, bank size is not a determinant of bank resilience.

Consistent with the findings by Amiry et al. (2018), the average bank already has reserves of customer inflows and surplus deposits, so they tend to be safe. At the country level, the results of our study show that when the political stability of the country is good, it will improve the financial resilience of banks. On the other hand, high political rights (voice and

accountability) reduce bank financial resilience. We conclude that the political stability of the country has an impact mainly by affecting the bank's capital adequacy and asset quality, income and profitability, and liquidity, and then the effect shifts to affect bank stability (Huang & Lin, 2021). Such is contrary to the findings of Bektas et al. (2022), that voice and accountability increase bank stability, although not as much as the effect of political stability on bank stability (Han et al., 2015). According to Han et al., (2015), the dimensions of voice and accountability in developing countries in Asia continue to deteriorate, in addition to controlling corruption and the rule of law. Meanwhile, the macro variable (GDPG) showed no significant positive correlation with bank financial resilience ($p > .01$, $p > .05$ and $p > .10$). This could be possible if the benefits of economic growth on bank stability have an effect in the long term (Thompson, 2021).

Additional and Robustness Test

As a robustness test, this study conducted another test using a different estimation method, namely, the OLS approach. The Chow and Hausman tests were carried out to determine the best model. The common effect method is most appropriate for Models 1 and 2, while the fixed effect method is used for Models 3 and 4. Table 4 describes the results of the regression with the common effect and the fixed effects, which in general show consistent results with the regression with the 2SLS approach. These four models have significant Prob (F-statistic) values (p value = .000) and Adjusted R-squared (adj. R^2) values for each model, of 0.1048, 0.1099, 0.2008 and 0.2059. This shows that the four models each have variations of 10.48 percent, 10.99 percent, 20.08 percent and 20.59 percent regarding the effect of the independent variables on resilience

Table 4 Result of model 1 and 2 (Common) and 3 and 4 (Fixed)

Variables	(1) Common	(2) Common	(3) Fixed	(4) Fixed
	VCRD	GCR	CAUSES	IMPACTS
	(SE)	(SE)	(SE)	(SE)
VCRD	0.9148 ***			
	(0.2917)			
GCR		0.5055 ***		
		(0.1501)		
CAUSESs			-0.3104	
			0.3938	
IMPACTSs				1.3119 ***
				0.2838
Size	-0.0032	-0.0046	0.8427 ***	0.7086 ***
	(0.0327)	(0.0320)	0.2876	0.2709
Lev	0.8915 **	0.8239 **	-2.5710	-2.2695
	(0.3804)	0.3556	1.8015	2.1967
NPL	6.5033 *	7.4668 **	9.2487 ***	8.6257 ***
	(3.7538)	3.7305	3.0113	2.6664
LDR	-0.6689	-0.6395	0.0222	-0.0959
	(0.5046)	0.4896	0.9578	1.0641
GDPG	0.3512	0.3176	0.1251	0.1427
	0.4017	0.4102	0.4432	0.5885
VA	1.0356	1.3639	8.5058 ***	7.4245 *
	1.9455	1.0197	2.2155	3.9601
PV	-4.6093 ***	-4.4632 **	-0.3563	-0.2991
	1.9455	1.9089	2.9288	4.7769
Observations	310	310	310	310
Adj. R-squared	0.1047	0.1098	0.2008	0.2059
Prob (F- statistic)	0.0000	0.0000	0.0000	0.0000

(the dependent variable). In Models 1, 2 and 4, resilience has a positive and significant relationship to VCRD, GCR and IMPACT, indicated by coefficient values of 0.9148, 0.5055, and 1.3119. That is, the higher the level of disclosure of cyber risk (total), the disclosure of cyber risk governance and the causes of cyber risk, the lower the bank's financial resilience. In this case, the bank's resilience value is close to zero, the higher the resilience. Meanwhile, the CAUSES coefficient value of -0.3104 was not significant ($p < .01$, $p < .05$ and $p < .10$) as shown in Model 3.

This study then conducted additional tests that aimed to analyze more deeply the results of the main regression, first grouping the levels of high and low cyber risk disclosures. This grouping is to investigate whether there is a difference in results between these two groups. According to Huang (2006), a bank can manipulate disclosed items or even not disclose at all to deceive investors. In addition, the level of cyber risk disclosure can explain bank cyber risk events. In categorizing the level of disclosure based on the calculation of the average disclosure, a disclosure level above the average indicates a high level of inhibition and vice versa. Furthermore, investigations into disclosures related to the causes and impacts of cyber risk based on this category cannot be carried out since, from the observations of this study, there are still many banks refusing to provide this information or there is no disclosure of this type. The test results are shown in Table 5.

The table above describes that there are differences in the influence of the two levels of grouping based on high disclosure (Panel A) and high disclosure (Panel B) samples. Cyber risk disclosure as a whole will have a significant positive effect on bank resilience only for samples where disclosure is below average. Meanwhile, disclosure of risk governance has a significant negative effect on bank resilience for a sample whose disclosure is above the average. This finding can be interpreted as high corporate governance disclosure indicates better cyber risk management thereby encouraging bank financial resilience.

Conclusion and Recommendation

Consistent with the Basel III reforms, it is imperative to build more resilient financial institutions. Disclosure of cyber risk by banks can be an important tool that allows managers to keep a company's finances in check.

Table 5 Regression results with 2SLS - two cyber risk disclosure groups

Variables	(1)	(2)	(1)	(2)
	High VCRD *(SE)*	High GCR *(SE)*	Low VCRD *(SE)*	Low GCR *(SE)*
VCRD	0.2459 *(0.4231)*		1.6568 ** (0.6398)	
GCR		-1.5031 ** *(0.6470)*		0.6124 *(3941)*
Size	-0.0458 *(0.0457)*	-0.1181 ** *(0.0589)*	-0.0338 *(0.0370)*	0.0092 *(0.0296)*
Lev	2.5118 *** (0.6330)	2.5027 *** (0.5062)	0.1864 (0.7584)	0.6633 (0.7450)
NPL	6.2657 (5.7565)	13.8741 ** (7.0288)	7.4204 *** (2.6129)	7.4163 *** (2.5179)
LDR	-2.7160 *** *(0.6285)*	-1.9869 *** *(0.7115)*	0.5097 *(0.4300)*	0.1396 *(0.3701)*
GDPG	-0.2058 (0.2685)	-0.4488 (0.3275)	0.6876 (0.3490)	0.5145 (0.4094)
VA	0.9958 (0.6929)	1.4722 * (0.7880)	0.0742 (0.8169)	1.5328 (1.0546)
PV	-6.1982 *** *(1.2569)*	-4.6322 *** *(1.5021)*	-0.5763 *(1.3521)*	-0.6799 *(1.1666)*
Observations	124	97	187	213
Adj. R-squared	0.4358	0.3514	0.2398	0.1062
Prob(F-statistic)	0.0000	0.0000	0.0000	0.0000

However, this research shows that total disclosure (cyber risk) and individual disclosure (governance and impact of cyber risk) reduce bank resilience, while the disclosure of the causes of cyber risk does not affect this performance. Our main results remain unchanged after performing a robustness analysis. Furthermore, the results of additional analysis show that there is a difference between the effect of this level of disclosure on bank resilience based on the group of banks that disclose above average and below average. This additional analysis implies which types of under disclosure affect the level of cyber risk disclosure.

There are implications for financial regulators, leading to two different policy conclusions. On the one hand, the study results show that banks under-disclose their cyber risk events. Therefore, ASEAN-4 financial regulators should continue to press for more disclosures as "events like these are important for markets". On the other hand, further disclosure could threaten or undermine the financial resilience of banks and the banks' ongoing efforts to shore up their cyber defenses. Banks must also provide essential services to the wider economy (mediators), the vulnerability of large banks to cyberattacks can threaten and disrupt these essential services—which has the potential for a detrimental contagion effect. Cyber risk disclosure thus appears to present a classic case for the growing importance of adequate regulatory intervention.

There are several limitations in this study. First, it is necessary for future research to pay attention to the weighting analysis for each disclosure item so that the design and results are more optimal. In addition, it is necessary to conduct in-depth interviews to find out information on cyber threats that may not be disclosed in the annual report because this information is still voluntary. Second, this study does not use other measurements in assessing the financial resilience of banks. For this reason, future studies can measure such using different methods (see Albert & Hee, 2012; Crossen et al., 2014; Hallegatte, 2014; Soufi et al., 2023). Third, the COVID-19 pandemic was not analysed in this study because the difference in resilience levels during the pandemic compared to the non-pandemic period was not significant (see Figure 1). Future research could extend the COVID-19 pandemic period (2020–2022) to analyse this effect. Finally, we have not considered the lag effect that could lead to the possible long-term effect of VCRD on financial resilience. The next study needs to elaborate on this to improve the analysis of the study results.

Conflict of Interest

The authors declare that there is no conflict of interest.

References

Albert, J, R., & Hee Ng, T. (2012). *Assessing the resilience of ASEAN banking systems: The case of Philippine institute for development studies*. ADB Working Paper Series on Regional Economic Integration. https://www.adb.org/publications/assessing-resilience-asean-banking-systems-case-philippines

Amir, E., Levi, S., & Livne, T. (2018). Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies*, *23*(3), 1177–1206. http://dx.doi.org/10.2139/ssrn.3136193

Amiry, M., Mohagheghnia, M. J., & Balavandi, A. (2018). Evaluating resilience of Iran's banking system and its affecting factors, *Monetary and Financial Economics*, *25*(15), 255–276. https://doi.org/10.22067/pm.v25i16.64030

Beatty, A., Cheng, L., & Zhang, H. (2019). Are risk factor disclosures still relevant? Evidence from market reactions to risk factor disclosures before and after the financial crisis. *Contemporary Accounting Research*, *36*(2), 805–838. https://doi.org/10.1111/1911-3846.12444

Bektas, E., Elbadri, M, & Molyneux, P. (2022). Do institutions, religion and the economic cycle impact bank stability in dual banking systems? *Journal of International Financial Management and Accounting*, *33*(2), 252–284. https://doi.org/10.1111/jifm.12146

Berkman, H., Jona, J., Lee, G., Soderstrom, N. (2018). Cybersecurity awareness and market valuations. *Journal of Accounting and Public Policy*, *37*(6), 508–526. https://doi.org/10.1016/j.jaccpubpol.2018.10.003

Brusset, X., & Teller, C. (2017). Supply chain capabilities, risks, and resilience. *International Journal of Production Economics*, *184*(C), 59–68. https://doi.org/10.1016/j.ijpe.2016.09.008

Buch, C. M., Eickmeier, S., & dan Prieto, E (2014). Macroeconomic factors and microlevel bank behavior. *Journal of Money, Credit and Banking*, *46*(4), 715–751. https://doi.org/10.1111/jmcb.12123

Budnik, K. B., & Bochmann, P. (2017). *Capital and liquidity buffers and the resilience of the banking system in the euro area*. (ECB Working Paper No. 2120). http://dx.doi.org/10.2139/ssrn.3095950

Campbell, J. L., Chen, H., Dhaliwal, D. S., Lu, H., & Steele, L. B. (2014). The information content of mandatory risk factor disclosures in corporate filings. *Review of Accounting Studies*, *19*(1), 396–455. https://doi.org/10.1007/s11142-013-9258-3

Cecchetti, S. G., & Tucker, P. M. W. (2016). *Is there macroprudential policy without international cooperation?* (Discussion Paper Series No. 11042). Centre for Economic Policy Research. https://ssrn.com/abstract=2717591

Chen, J., Henry, E., Jiang, X. (2022). Is Cybersecurity risk factor disclosure informative? Evidence from disclosures following a data breach. *Journal of Business Ethics*, 187, 199–224. https://doi.org/10.1007/s10551-022-05107-z

Clark, L. A., & Watson, D. (1995). Constructing validity: Basic issues in objective scale development. *Psychological Assessment*, *7*(3), 309–319. https://doi.org/10.1037/1040-3590.7.3.309

Crossen, C., Liang, X., Protsyk, A., & Zhang, J. (2014). *Measuring the banking system's resilience*. https://www.moodysanalytics.com/-/media/whitepaper/2014/2014-19-11- Measuring-the-Banking-System-Final-Report.pdf

European Central Bank-ECB. (2005). *Bank market discipline*. Monthly Bulletin for February 2005. https://www.ecb.europa.eu/pub/pdf/mobu/mb200502en.pdf

European Banking Authority-EBA. (2020). *Annual report 2020*. https://www.eba.europa.eu/sites/default/files/document_library/

Gensler, C. G. (2022). Statement on proposal for mandatory cybersecurity disclosures. https://www.sec.gov/newsroom/speeches-statements/gensler-cybersecurity-20220309.

Ghosh, R., & Saima, F. N. (2021). Resilience of commercial banks of Bangladesh to the shocks caused by COVID-19 pandemic: An application of MCDM-based approaches. *Asian Journal of Accounting Research*, *6*(3), 281–295. https://doi.org/10.1108/AJAR-10-2020-0102

Gropp, R., & Moerman, G. (2004). Measurement of contagion in bank equity prices. *Journal of International Money and Finance*, *23*, 405–459. https://doi.org/10.1016/j.jimonfin.2004.01.005

Guettafi, S., & Laib, Y. (2016). Resilience and stability of Algeria's financial system towards– resilience versus stability-approach. *Journal of Economics*, *4*(1), 78–90. https://doi.org/10.15640/jeds.v4n1a8

Hallegatte, S. (2014). *Economic resilience: Definition and measurement*. (Policy Research Working Paper, No. 6852). https://documents1.worldbank.org/curated/en/350411468149663792/pdf/WPS6852.pdf

Han, R., & Melecky, M. (2013). *Financial inclusion for financial stability: Access to bank deposits and the growth of deposits in the global financial crisis* (World Bank Policy Research Working Paper No. 6577). World Bank. http://documents.worldbank.org/curated/en/850681468325448388/Financial-inclusion-for-financial-stability-access-to-bank-deposits-and-the-growth-of-deposits-in-the-Global-Financial-Crisis

Han, X., Khan, H. & Zhuang. J. (2015). *Do governance indicators explain growth performance? A cross-country analysis*. *In Governance in developing Asia: Public service delivery and empowerment*. Edward Elgar Publishing. https://doi.org/10.4337/9781784715571.

Havakhor, T., Rahman, M. S., & Zhang, T. (2021). *Disclosure of cybersecurity investments and the cost of capital*. https://ssrn.com/abstract=3553470

Hilary, G., Segal, B., & Zhang, M. H. (2016). *Cyber-risk disclosure: Who cares?. Georgetown McDonough School of Business* (Research Paper No. 2852519). http://dx.doi.org/10.2139/ssrn.2852519

Histen, M. J. (2022). Taking information seriously: A firm-side interpretation of risk factor disclosure. *International Advance in Economic Research*, *28*, 119–131. https://doi.org/10.1007/s11294-022-09856-5.

Hope, O. K., Hu, D., & Lu, H. (2016). The benefits of specific risk-factor disclosures. *Review of Accounting Studies*, *21*(4), 1005–1045. https://doi.org/10.1007/s11142-016-9371-1

Huang, R. (2006). *Bank disclosure index: Global assessment of bank disclosure practices*. World Bank Group. http://documents.worldbank.org/curated/en/611351468159909764/Bank-disclosure-index-global-assessment-of-bank-disclosure-practices

Huang, J., & Lin, H. (2021). Country risk and bank stability. *Romanian Journal of Economic Forecasting*, *24*(3), 72–96. https://ipe.ro/new/rjef/rjef3_2021/rjef3_2021p72-96.pdf

Jiang, W., Legoria, J., Reichelt, K. J., & Waltom, S. (2022). Firm use of cybersecurity risk disclosures. *Journal of Information Systems*, *36*(1), 151–180. https:/ /doi.org/10.2308/ISYS-2020-067

Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*, *139*(3), 719–749. https://doi.org/10.1016/j.jfineco.2019.05.019

Kaendera, S. & Leigh, L. (2021). *Five things to know about Thailand's economy and COVID-19*. IMF Asia and Pacific Department. https://www.imf.org/en/News/Articles/2021/06/21/na062121-5-things-to-know-about-thailands-economy-and-covid-19.

Karyani, E., Dewo, S. A., Frensidy, B., & Santoso, W. (2019). Role of risk governance in promoting operational risk disclosure and performance: An ASEAN-5 banking perspective. *International Journal of Business and Society*, *20*(3), 1218–1235.

Karyani, E., Dewo, S. A., Santoso, W., & Frensidy, B. (2020). Risk governance and bank profitability in ASEAN-5: A comparative and empirical study. *International Journal of Emerging Markets*, *15*(5), 949–969. https://doi.org/10.1108/IJOEM-03-2018-0132

Karyani, E., Kolade, O., & Dewo, S. A. (2021). Risk governance, market competition and operational risk disclosure quality: A Study of the ASEAN-5 Banking Sector. *Journal of Operational Risk*, *16*(2), 61–86. https://doi.org/10.21314/JOP.2021.004

KPMG. (2020). *Financial resilience in banking: A balancing act*. https://assets.kpmg/content/dam/kpmg/xx/pdf/2020/12/financial-resilience-in-banking.pdf

Leuz, C., & Wysocki, P. D. (2016). The economics of disclosure and financial reporting regulation: Evidence and suggestions for future research, *Journal of Accounting research*, *54*, 525–626. https://doi.org/10.1111/1475-679X.12115

Li, H., No, W. G., & Wang, T. (2018). SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems*, *30*, 40–55. https://doi.org/10.1016/j.accinf.2018.06.003

Maheswaran, M., & Rao, D. N. (2014). Stress test for risk assessment under Basel framework applied in banking industry. *Risk Governance and Control: Financial Markets and Institutions*, *4*(3), 25–29. https://doi.org/10.22495/rgcv4i3art3

McDonough, W. J. (2003). Promoting financial resilience. *Cato Journal*, *23*(1), 11–21. https://www.bis.org/review/r021028b.pdf

Merton, R. C. (1974). On the pricing of corporate debt: The risk structure of interest rates. *The Journal of Finance*, *29*(2), 449–470. https://doi.org/10.1111/j.1540-6261.1974.tb03058.x

Moretti, M., Dobler, M. C., & Chavarri, A. P. (2020). *Managing systemic banking crises: New lessons and lessons relearned*. Monetary and Capital Markets Department, International Monetary Fund.

Nkundabanyanga, S. K., Mugumya, E., Nalukenge, I., Muhwezi, M., & Najjemba, G. M. (2020). Firm characteristics, innovation, financial resilience and survival of financial institutions. *Journal of Accounting in Emerging Economies*, *10*(1), 48–73. https://doi.org/10.1108/JAEE-08-2018-0094

O'Neill, B, (2011). *Steps toward financial resilience*. https://njaes.rutgers.edu/sshw/message/message.php?p=Finance&m=194

Patra, B, & Padhi, P. (2020). Resilience of Indian banks: Macroeconomic stress test modeling for Indian banks. *Journal of Public Affairs, 22*, e2350. https://doi.org/10.1002/pa.2350

Ruza, C., de la Cuesta-González, M., & Paredes-Gazquez, J. (2019). Banking system resilience: An empirical appraisal. *Journal of Economic Studies*, *46*(6), 1241–1257.

Salter, A. W., & Tarko, V. (2017). Governing the financial system: A theory of financial resilience. (Mercatus Working Paper, November 2017). http://dx.doi.org/10.2139/ssrn.3084352

Skinner, C. P. (2019). *Bank disclosures of cyber exposure*. Iowa Law Review, *105*. https://ssrn.com/abstract=3519159

Soufi, H. R., Esfahanipour, A., & Shiraz, M. A. (2023). A Quantitative measure for financial resilience of firms: Evidence from Tehran stock exchange. *Scientia Iranica*, *30*(1), 302–317. https://doi.org10.24200/SCI.2021.55845.4433

Tariq, N. (2018). Impact of cyberattacks on financial institutions. *Journal of Internet Banking and Commerce*, *23*(2), 1–11. https://smartlib.umri.ac.id/assets/uploads/files/24c10-impact-of-cyberattacks-on-financial-institutions.pdf

Thompson, F. (2021) The effect of macroeconomic variables on the asset positions and financial performance of Non-Banking Financial Institutions (NBFIs) in Jamaica. *Journal of Business and Management*, *9*, 1424–1445. https://doi.org/10.4236/ojbm.2021.93076.

Triggs, A., Kacaribu, F., & Wang, J. (2019). Risks, resilience, and reforms: Indonesia's financial system in 2019. *Bulletin of Indonesian Economic Studies*, *55*(1), 1–27. https://doi.org/10.1080/00074918.2019.1592644

Vallascas, F., & Keasey, K. (2012). Bank resilience to systemic shocks and the stability of banking systems: Small is beautiful. *Journal of International Money and Finance*, *31*(6), 1745–1776. https://doi.org/10.1016/j.jimonfin.2012.03.011